2011 情財第 399 号

情報セキュリティ対策基盤整備事業

「電子政府推奨暗号の実装」

報告書

平成 24 年 12 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

1. 概要

図 1.1 に示すように，サイドチャネル攻撃用標準評価ボード SASEBO-GII 上の FPGA Virtex-5 上に，電子政府推奨暗号リスト掲載のアルゴリズムのうち，下記の 5 種類の 128bit ブロック暗号，および 2 種類のストリーム暗号を実装し，実機動作検証および，CAD ツールによる性能評価を行った．

・AES (ブロック長 128 ビット，鍵長 128 ビット)
・Camellia (ブロック長 128 ビット，鍵長 128 ビット)
・CIPHERUNICORN-A (ブロック長 128 ビット，鍵長 128 ビット)
・Hierocrypt-3 (ブロック長 128 ビット，鍵長 128 ビット)
・SC2000 (ブロック長 128 ビット，鍵長 128 ビット)
・MULTI-S01 (ブロック長 64 ビット，鍵長 256 ビット，IV 長 256 ビット)
・MUGI (ブロック長 64 ビット，鍵長 128 ビット，IV 長 256 ビット)

SASEBO-GII 上の FPGA Spartan-3A に実装した USB インタフェースおよび制御回路は，IPA から提供される「電子政府推奨暗号用ハードウェア評価環境」をベースに，各アルゴリズムの入出力データサイズ/入出力タイミング/処理サイクル数等を考慮した変更を適宜加えており，Windows PC の USB ポートとボード上の USB コントローラを接続することで，各暗号回路を制御する．Windows PC 上の制御ソフトウェアも上記「電子政府推奨暗号用ハードウェア評価環境」をベースに開発し，アルゴリズムごとのインタフェースの違いを吸収できるよう変更を加えている．

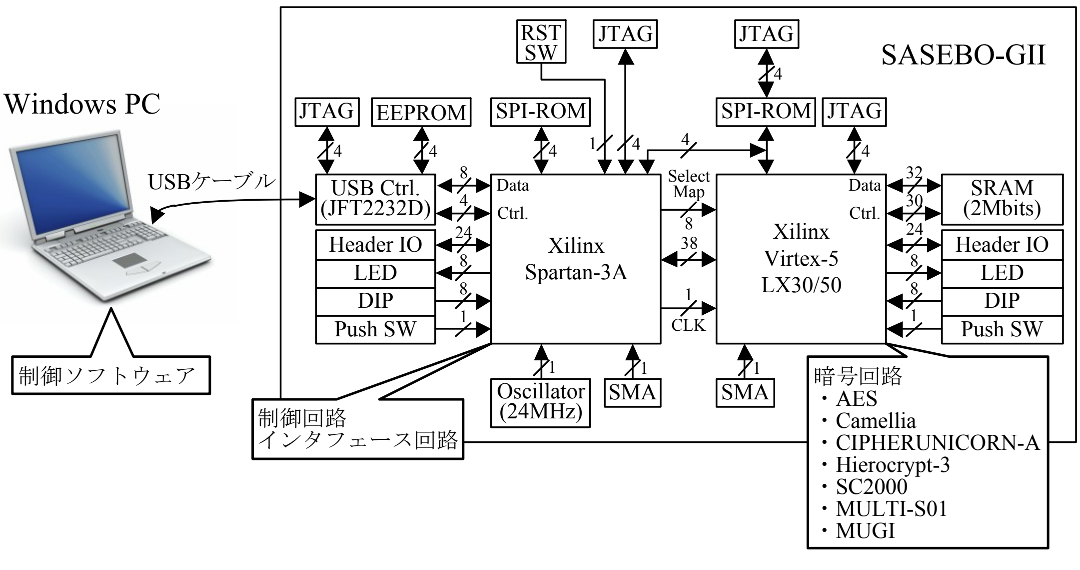


図 1.1 システム構成

各暗号回路は処理速度を優先するため，内部データバス幅を可能な限り広く取り，クリティカルパスの速度に大きな影響を与える S-box 等の非線形関数はルックアップテーブル(LUT)実装とした．また，ブロック暗号は，ランダム化関数ブロックを 1 ラウンド分用意して反復利用するループアーキテクチャを採用している．

各暗号回路およびインタフェース回路はVerilog-HDL言語で記述し，ISE WebPACK Version 12.4によってSASEBO-GIIのFPGA Viretex-5上への実装および性能評価を行った．SASEBO-GII上の実装のターゲット動作周波数は 24MHz であるが，CIPHERUNICORN-A は論理合成の結果，24MHz を満たすことができなかったので，インタフェース FPGA Spartan-3 の動作周波数を半分の12MHz とする制御回路も設計・実装した．ただし，FPGA のスペックは動作マージンを含んでいるため，手元の実機ではCIPHERUNICORN-Aも24MHzで動作している．

表1.1に，納品物のDVDメディアDISC1におさめたファイルの一覧を示す．また暗号回路と制御回路のソースファイルは納品物ではないが，表1.2に示すように“参考情報”としてDISC2におさめている．各メディアのディレクトリの概要は下記の通りである．

●DISC1

<文書>ディレクトリには，本報告書，評価結果，プログラム取扱説明書の pdf ファイルが納められている．

<設計情報>ディレクトリは，CAD サマリを含む設計情報として，Qualtus II および，ISE WebPACK の論路合成レポートが納められている．Qualtus II では Cyclone III および Stratix III に対して，各暗号回路のコアモジュールのみを論理合成している．それに対して，ISE WebPACK では Spartan-3,Spartan-6,Virtex-5,Virtex-6に対してコアモジュールのみ，そして消費電力評価のためコアモジュール+インタフェース回路の2種類の論理合成を行った．なお，Hieroctypt-3とMULTI-S01は spartan-3 ではリソース不足のため，電力レポートの pwr ファイルと，タイミングレポートの twr ファイルは存在しない．

<コンフィギュレーションデータ>ディレクトリの下には二つのディレクトリがあり，<Virtex-5>には各暗号回路のビットストリームファイル“暗号名.bit” と SPI ROM ファイル“暗号名.mcs”が納められている．また<Spartan-3>ディレクトリには，制御回路のコンフィギュレーションデータが納められている．“FPGA2.bit” と “FPGA2.mcs”は，(独)産業技術総合研究所情報セキュリティ研究センターが開発した「電子政府推奨暗号用ハードウェア評価環境」のソースファイルをそのまま論理合成したものである．しかし，CIPHERUNICORN-Aは論理合成の結果SASEBO-GIIの標準動作周波数24MHzを満たすことができなかったため（実機では動作している），半分の12MHzで動作させるために修正を施した FPGA2_12MHz.bit” と “FPGA2_12MHz.mcs”もおさめた．

<制御プログラム>ディレクトリは暗号回路の制御ソフトウェア関連のファイルが納められている．“algorithm_test.cs”は上記の評価環境として公開されている制御ソフトウェアを一部修正しており，そのWindows上の実行ファイルが “algorithm_test.exe” となる．“暗号名.txt”は“algorithm_test.exe”が読み込むスクリプトファイルで，各暗号外路制御用のコマンドやのテストベクタが記述されている．使用法は「4.2 制御ソフトウェアのインタフェース」を参照されたい．また，“FTD2XX_NET.dll” と “FTD2XX_NET.xml” は FTDI (Future Technology Devices International)社から公開されている（http://www.ftdichip.com/Support/SoftwareExamples/CodeExamples/CSharp.htm），USBコントローラの制御に用いるライブラリファイルである．

●DISC2

<回路ソースファイル>ディレクトリの下の<Virtex-5>ディレクトリには，さらに各暗号名のディレクトリが存在し，“FPGA1_暗号名.v” をトップとする Verilog-HDL ソース群（“FPGA1_暗号名.v”, “暗号名.ucf”, “暗号名.v”, “lbus_if.v”）がおさめられている．なお MULTI-S01 だけは，それら 4 つのソース以外に “PANAMA.v” が必要となる．“暗号名.v”が暗号回路コアモジュールで，“暗号名_tb.v”はそのテストベンチである．“暗号名.ucf”は Virtex-5 用のピンアサイン用ファイルであり，“lbus_if.v”はインタフェース回路である．なお，“暗号名.ucf”, “FPGA1_暗号名.v”, そして“lbus_if.v”は，「電子政府推奨暗号用ハードウェア評価環境」をそのまま，もしくは暗号アルゴリズムに合わせて修正したものである．

<Spartan-3>ディレクトリには「電子政府推奨暗号用ハードウェア評価環境」の制御回路を CIPHERUNICORN-A 用に 12MHz で動作させるために修正したソースファイル “chip_sasebo_gii_ctrl_12MHz.v”が納められている．

表 1.1 DISC 1 の内容

<文書>				
	報告書.pdf			報告書 pdf ファイル
	報告書.word			報告書 Word ファイル
	評価結果.pdf			評価結果 pdf ファイル
	評価結果.word			評価結果 Word ファイル
	プログラム取扱説明書.pdf			制御プログラム取扱説明書 pdf ファイル
	プログラム取扱説明書.sord			制御プログラム取扱説明書 Word ファイル
<設計情報>				
	<Cyclone III>			
		<AES>		
			AES.flow	Qualtus II flow report
			AES.map	Qualtus II analysis & synthesis report
		<Camellia>		
			Camellia.flow	Qualtus II flow report
			Camellia.map	Qualtus II analysis & synthesis report
		<CIPHERUNICORN-A>		
			CIPHERUNICORN_A.flow	Qualtus II flow report
			CIPHERUNICORN_A.map	Qualtus II analysis & synthesis report
		< Hierocrypt-3 >		
			Hierocrypt_3.flow	Qualtus II flow report
			Hierocrypt_3.map	Qualtus II analysis & synthesis report
		<MUGI>		
			MUGI.flow	Qualtus II flow report
			MUGI.map	Qualtus II analysis & synthesis report
		<MULTI-S01>		
			MULTI_S01.flow	Qualtus II flow report
			MULTI_S01.map	Qualtus II analysis & synthesis report
		<SC2000>		
			SC2000.flow	Qualtus II flow report
			SC2000.map	Qualtus II analysis & synthesis report
	<Stratix III>			
		<AES>		
			AES.flow	Qualtus II flow report
			AES.map	Qualtus II analysis & synthesis report
		<Camellia>		
			Camellia.flow	Qualtus II flow report
			Camellia.map	Qualtus II analysis & synthesis report
		<CIPHERUNICORN-A>		
			CIPHERUNICORN_A.flow	Qualtus II flow report
			CIPHERUNICORN_A.map	Qualtus II analysis & synthesis report

	< Hierocrypt-3 >			
			Hierocrypt_3.flow	Qualtus II flow report
			Hierocrypt_3.map	Qualtus II analysis & synthesis report
	<MUGI>			
			MUGI.flow	Qualtus II flow report
			MUGI.map	Qualtus II analysis & synthesis report
	<MULTI-S01>			
			MULTI_S01.flow	Qualtus II flow report
			MULTI_S01.map	Qualtus II analysis & synthesis report
	<SC2000>			
			SC2000.flow	Qualtus II flow report
			SC2000.map	Qualtus II analysis & synthesis report
<Spartan-3>				
	<AES>			
		<コア>		
			AES.summary.html	ISE synthesis summary
			AES.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_AES.summary.html	ISE synthesis summary
			FPGA1_AES.syr	ISE synthesis report
			FPGA1_AES.map.mrp	ISE mapping report
			FPGA1_AES.pwr	ISE power analysis report
			FPGA1_AES.twr	ISE timing report
	<Camellia>			
		<コア>		
			Camellia.summary.html	ISE synthesis summary
			Camellia.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_Camellia.summary.html	ISE synthesis summary
			FPGA1_Camellia.syr	ISE synthesis report
			FPGA1_Camellia.map.mrp	ISE mapping report
			FPGA1_Camellia.pwr	ISE power analysis report
			FPGA1_Camellia.twr	ISE timing report
	<CIPHERUNICORN-A>			
		<コア>		
			CIPHERUNICORN_A.summary.html	ISE synthesis summary
			CIPHERUNICORN_A.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_CIPHERUNICORN_A.summary.html	ISE synthesis summary
			FPGA1_CIPHERUNICORN_A.syr	ISE synthesis report
			FPGA1_CIPHERUNICORN_A.map.mrp	ISE mapping report
			FPGA1_CIPHERUNICORN_A.pwr	ISE power analysis report
			FPGA1_CIPHERUNICORN_A.twr	ISE timing report
	<Hierocrypt-3>			
		<コア>		
			Hierocrypt_3.summary.html	ISE synthesis summary
			Hierocrypt_3.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_Hierocrypt_3.summary.html	ISE synthesis summary
			FPGA1_Hierocrypt_3.syr	ISE synthesis report
			FPGA1_Hierocrypt_3.map.mrp	ISE mapping report
	<MUGI>			
		<コア>		
			MUGI.summary.html	ISE synthesis summary
			MUGI.syn	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_MUGI.summary.html	ISE synthesis summary
			FPGA1_MUGI.syr	ISE synthesis report
			FPGA1_MUGI.map.mrp	ISE mapping report
			FPGA1_MUGI.pwr	ISE power analysis report
			FPGA1_MUGI.twr	ISE timing report
	<MULTI-S01>			
		<コア>		
			MULTI_S01.summary.html	ISE synthesis summary
			MULTI_S01.syr	ISE synthesis report
		<コア+インタフェース>		

			File	Description
			FPGA1_MULTI_S01.summary.html	ISE synthesis summary
			FPGA1_MULTI_S01.syr	ISE synthesis report
			FPGA1_MULTI_S01.map.mrp	ISE mapping report
	<SC2000>			
		<コア>		
			SC2000.summary.html	ISE synthesis summary
			SC2000.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_SC2000.summary.html	ISE synthesis summary
			FPGA1_SC2000.syr	ISE synthesis report
			FPGA1_SC2000.map.mrp	ISE mapping report
			FPGA1_SC2000.pwr	ISE power analysis report
			FPGA1_SC2000.twr	ISE timing report
<Spartan-6>				
	<AES>			
		<コア>		
			AES.summary.html	ISE synthesis summary
			AES.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_AES.summary.html	ISE synthesis summary
			FPGA1_AES.syr	ISE synthesis report
			FPGA1_AES.map.mrp	ISE mapping report
			FPGA1_AES.pwr	ISE power analysis report
			FPGA1_AES.twr	ISE timing report
	<Camellia>			
		<コア>		
			Camellia.summary.html	ISE synthesis summary
			Camellia.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_Camellia.summary.html	ISE synthesis summary
			FPGA1_Camellia.syr	ISE synthesis report
			FPGA1_Camellia.map.mrp	ISE mapping report
			FPGA1_Camellia.pwr	ISE power analysis report
			FPGA1_Camellia.twr	ISE timing report
	<CIPHERUNICORN-A>			
		<コア>		
			CIPHERUNICORN_A.summary.html	ISE synthesis summary
			CIPHERUNICORN_A.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_CIPHERUNICORN_A.summary.html	ISE synthesis summary
			FPGA1_CIPHERUNICORN_A.syr	ISE synthesis report
			FPGA1_CIPHERUNICORN_A.map.mrp	ISE mapping report
			FPGA1_CIPHERUNICORN_A.pwr	ISE power analysis report
			FPGA1_CIPHERUNICORN_A.twr	ISE timing report
	<Hierocrypt-3>			
		<コア>		
			Hierocrypt_3.summary.html	ISE synthesis summary
			Hierocrypt_3.syr	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_Hierocrypt_3.summary.html	ISE synthesis summary
			FPGA1_Hierocrypt_3.syr	ISE synthesis report
			FPGA1_Hierocrypt_3.map.mrp	ISE mapping report
			FPGA1_Hierocrypt_3.pwr	ISE power analysis report
			FPGA1_Hierocrypt_3.twr	ISE timing report
	<MUGI>			
		<コア>		
			MUGI.summary.html	ISE synthesis summary
			MUGI.syn	ISE synthesis report
		<コア+インタフェース>		
			FPGA1_MUGI.summary.html	ISE synthesis summary
			FPGA1_MUGI.syr	ISE synthesis report
			FPGA1_MUGI.map.mrp	ISE mapping report
			FPGA1_MUGI.pwr	ISE power analysis report
			FPGA1_MUGI.twr	ISE timing report
	<MULTI-S01>			
		<コア>		

				MULTI_S01.summary.html	ISE synthesis summary
				MULTI_S01.syr	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_MULTI_S01.summary.html	ISE synthesis summary
				FPGA1_MULTI_S01.syr	ISE synthesis report
				FPGA1_MULTI_S01.map.mrp	ISE mapping report
				FPGA1_MULTI_S01.pwr	ISE power analysis report
				FPGA1_MULTI_S01.twr	ISE timing report
		<SC2000>			
			<コア>		
				SC2000.summary.html	ISE synthesis summary
				SC2000.syr	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_SC2000.summary.html	ISE synthesis summary
				FPGA1_SC2000.syr	ISE synthesis report
				FPGA1_SC2000.map.mrp	ISE mapping report
				FPGA1_SC2000.pwr	ISE power analysis report
				FPGA1_SC2000.twr	ISE timing report
	<Virtex-5>				
		<AES>			
			<コア>		
				AES.summary.html	ISE synthesis summary
				AES.syr	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_AES.summary.html	ISE synthesis summary
				FPGA1_AES.syr	ISE synthesis report
				FPGA1_AES.map.mrp	ISE mapping report
				FPGA1_AES.pwr	ISE power analysis report
				FPGA1_AES.twr	ISE timing report
		<Camellia>			
			<コア>		
				Camellia.summary.html	ISE synthesis summary
				Camellia.syr	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_Camellia.summary.html	ISE synthesis summary
				FPGA1_Camellia.syr	ISE synthesis report
				FPGA1_Camellia.map.mrp	ISE mapping report
				FPGA1_Camellia.pwr	ISE power analysis report
				FPGA1_Camellia.twr	ISE timing report
		<CIPHERUNICORN-A>			
			<コア>		
				CIPHERUNICORN_A.summary.html	ISE synthesis summary
				CIPHERUNICORN_A.syr	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_CIPHERUNICORN_A.summary.html	ISE synthesis summary
				FPGA1_CIPHERUNICORN_A.syr	ISE synthesis report
				FPGA1_CIPHERUNICORN_A.map.mrp	ISE mapping report
				FPGA1_CIPHERUNICORN_A.pwr	ISE power analysis report
				FPGA1_CIPHERUNICORN_A.twr	ISE timing report
		<Hierocrypt-3>			
			<コア>		
				Hierocrypt_3.summary.html	ISE synthesis summary
				Hierocrypt_3.syr	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_Hierocrypt_3.summary.html	ISE synthesis summary
				FPGA1_Hierocrypt_3.syr	ISE synthesis report
				FPGA1_Hierocrypt_3.map.mrp	ISE mapping report
				FPGA1_Hierocrypt_3.pwr	ISE power analysis report
				FPGA1_Hierocrypt_3.twr	ISE timing report
		<MUGI>			
			<コア>		
				MUGI.summary.html	ISE synthesis summary
				MUGI.syn	ISE synthesis report
			<コア+インタフェース>		

				FPGA1_MUGI.summary.html FPGA1_MUGI.syr FPGA1_MUGI.map.mrp FPGA1_MUGI.pwr FPGA1_MUGI.twr	ISE synthesis summary ISE synthesis report ISE mapping report ISE power analysis report ISE timing report
		<MULTI-S01>			
			<コア>		
				MULTI_S01.summary.html MULTI_S01.syr	ISE synthesis summary ISE synthesis report
			<コア+インタフェース>		
				FPGA1_MULTI_S01.summary.html FPGA1_MULTI_S01.syr FPGA1_MULTI_S01.map.mrp FPGA1_MULTI_S01.pwr FPGA1_MULTI_S01.twr	ISE synthesis summary ISE synthesis report ISE mapping report ISE power analysis report ISE timing report
		<SC2000>			
			<コア>		
				SC2000.summary.html SC2000.syr	ISE synthesis summary ISE synthesis report
			<コア+インタフェース>		
				FPGA1_SC2000.summary.html FPGA1_SC2000.syr FPGA1_SC2000.map.mrp FPGA1_SC2000.pwr FPGA1_SC2000.twr	ISE synthesis summary ISE synthesis report ISE mapping report ISE power analysis report ISE timing report
	<Virtex-5>				
		<AES>			
			<コア>		
				AES.summary.html AES.syr	ISE synthesis summary ISE synthesis report
			<コア+インタフェース>		
				FPGA1_AES.summary.html FPGA1_AES.syr FPGA1_AES.map.mrp FPGA1_AES.pwr FPGA1_AES.twr	ISE synthesis summary ISE synthesis report ISE mapping report ISE power analysis report ISE timing report
		<Camellia>			
			<コア>		
				Camellia.summary.html Camellia.syr	ISE synthesis summary ISE synthesis report
			<コア+インタフェース>		
				FPGA1_Camellia.summary.html FPGA1_Camellia.syr FPGA1_Camellia.map.mrp FPGA1_Camellia.pwr FPGA1_Camellia.twr	ISE synthesis summary ISE synthesis report ISE mapping report ISE power analysis report ISE timing report
		<CIPHERUNICORN-A>			
			<コア>		
				CIPHERUNICORN_A.summary.html CIPHERUNICORN_A.syr	ISE synthesis summary ISE synthesis report
			<コア+インタフェース>		
				FPGA1_CIPHERUNICORN_A.summary.html FPGA1_CIPHERUNICORN_A.syr FPGA1_CIPHERUNICORN_A.map.mrp FPGA1_CIPHERUNICORN_A.pwr FPGA1_CIPHERUNICORN_A.twr	ISE synthesis summary ISE synthesis report ISE mapping report ISE power analysis report ISE timing report
		<Hierocrypt-3>			
			<コア>		
				Hierocrypt_3.summary.html Hierocrypt_3.syr	ISE synthesis summary ISE synthesis report
			<コア+インタフェース>		
				FPGA1_Hierocrypt_3.summary.html FPGA1_Hierocrypt_3.syr FPGA1_Hierocrypt_3.map.mrp FPGA1_Hierocrypt_3.pwr FPGA1_Hierocrypt_3.twr	ISE synthesis summary ISE synthesis report ISE mapping report ISE power analysis report ISE timing report
		<MUGI>			

			<コア>		
				MUGI.summary.html	ISE synthesis summary
				MUGI.syn	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_MUGI.summary.html	ISE synthesis summary
				FPGA1_MUGI.syr	ISE synthesis report
				FPGA1_MUGI.map.mrp	ISE mapping report
				FPGA1_MUGI.pwr	ISE power analysis report
				FPGA1_MUGI.twr	ISE timing report
		<MULTI-S01>			
			<コア>		
				MULTI_S01.summary.html	ISE synthesis summary
				MULTI_S01.syr	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_MULTI_S01.summary.html	ISE synthesis summary
				FPGA1_MULTI_S01.syr	ISE synthesis report
				FPGA1_MULTI_S01.map.mrp	ISE mapping report
				FPGA1_MULTI_S01.pwr	ISE power analysis report
				FPGA1_MULTI_S01.twr	ISE timing report
		<SC2000>			
			<コア>		
				SC2000.summary.html	ISE synthesis summary
				SC2000.syr	ISE synthesis report
			<コア+インタフェース>		
				FPGA1_SC2000.summary.html	ISE synthesis summary
				FPGA1_SC2000.syr	ISE synthesis report
				FPGA1_SC2000.map.mrp	ISE mapping report
				FPGA1_SC2000.pwr	ISE power analysis report
				FPGA1_SC2000.twr	ISE timing report
<コンフィギュレーションデータ>					
	<Virtex-5>				
		<AES>			
			AES.bit		Virtex-5 bit-stream file
			AES.mcs		Virtex-5 PROM file
		<Camellia>			
			Camellia.bit		Virtex-5 bit-stream file
			Camellia.mcs		Virtex-5 PROM file
		<CIPHERUNICORN-A>			
			CIPHERUNICORN_A.bit		Virtex-5 bit-stream file
			CIPHERUNICORN_A.mcs		Virtex-5 PROM file
		< Hierocrypt-3 >			
			Hierocrypt_3.bit		Virtex-5 bit-stream file
			Hierocrypt_3.mcs		Virtex-5 PROM file
		<MUGI>			
			MUGI.bit		Virtex-5 bit-stream file
			MUGI.mcs		Virtex-5 PROM file
		<MULTI-S01>			
			MULTI_S01.bit		Virtex-5 bit-stream file
			MULTI_S01.mcs		Virtex-5 PROM file
		<SC2000>			
			SC2000.bit		Virtex-5 bit-stream file
			SC2000.mcs		Virtex-5 PROM file
	<Spartan-3>				
		FPGA2.bit			Spartan-3 bit-stream file (24MHz 版)
		FPGA2.mcs			Spartan-3 PROM file (24MHz 版)
		FPGA2_12MHz.bit			Spartan-3 bit-stream file (12MHz 版)
		FPGA2_12MHz.mcs			Spartan-3 PROM file (12MHz 版)
<制御プログラム>					
	algorithm_test.cs				PC 上の制御プログラムソースファイル
	algorithm_test.exe				PC 上の制御プログラム実行ファイル
	FTD2XX_NET.dll				USB 制御用 DLL ファイル
	FTD2XX_NET.xml				USB 制御用 XML ファイル
	AES.txt				AES 用スクリプトファイル
	Camellia.txt				Camellia 用スクリプトファイル
	CIPHERUNICORN-A.txt				CIPHERUNICORN-A 用スクリプトファイル
	Hierocrypt-3.txt				Hierocrypt-3 用スクリプトファイル
	MUGI.txt				MUGI 用スクリプトファイル

	MULTI-S01.txt	MULTI-S01 用スクリプトファイル
	SC2000.txt	SC2000 用スクリプトファイル

表 1.2　DISC2 の内容

〈回路ソースファイル〉			
	<Virtex-5>		
	<AES>		
		AES.ucf	I/O ピン指定ファイル
		AES.v	暗号回路コアソースファイル
		AES_tb.v	暗号回路コアテストベンチ
		FPGA1_AES.v	号回路トップモジュールソースファイル
		lbus_if.v	インタフェース回路ソースファイル
	<Camellia>		
		Camellia.ucf	I/O ピン指定ファイル
		Camellia.v	暗号回路コアソースファイル
		Camellia_tb.v	暗号回路コアテストベンチ
		FPGA1_Camellia.v	号回路トップモジュールソースファイル
		lbus_if.v	インタフェース回路ソースファイル
	<CIPHERUNICORN-A>		
		CIPHERUNICORN-A.ucf	I/O ピン指定ファイル
		CIPHERUNICORN-A.v	暗号回路コアソースファイル
		CIPHERUNICORN-A_tb.v	暗号回路コアテストベンチ
		FPGA1_ CIPHERUNICORN-A.v	号回路トップモジュールソースファイル
		lbus_if.v	インタフェース回路ソースファイル
	< Hierocrypt-3 >		
		Hierocrypt-3.ucf	I/O ピン指定ファイル
		Hierocrypt-3.v	暗号回路コアソースファイル
		Hierocrypt-3.v	暗号回路コアテストベンチ
		FPGA1_ Hierocrypt-3.v	号回路トップモジュールソースファイル
		lbus_if.v	インタフェース回路ソースファイル
	<MUGI>		
		MUGI.ucf	I/O ピン指定ファイル
		MUGI.v	暗号回路コアソースファイル
		MUGI_tb.v	暗号回路コアテストベンチ
		FPGA1_MUGI.v	号回路トップモジュールソースファイル
		lbus_if.v	インタフェース回路ソースファイル
	<MULTI-S01>		
		MULTI-S01.ucf	I/O ピン指定ファイル
		MULTI-S01.v	暗号回路コアソースファイル
		MULTI-S01_tb.v	暗号回路コアテストベンチ
		FPGA1_MULTI-S01.v	号回路トップモジュールソースファイル
		lbus_if.v	インタフェース回路ソースファイル
	<SC2000>		
		SC2000.ucf	I/O ピン指定ファイル
		SC2000.v	暗号回路コアソースファイル
		SC2000_tb.v	暗号回路コアテストベンチ
		FPGA1_SC2000.v	号回路トップモジュールソースファイル
		lbus_if.v	インタフェース回路ソースファイル
	<Spartan-3>		
		chip_sasebo_gii_ctrl_12MHz.v	Spartan-3 用制御回路（12MHz 版)

表 1.3 は上記"暗号名.v"ファイルの暗号マクロブロックに共通の I/O ポートである. なお, データ入出力のタイミングは暗号アルゴリズム毎に異なっている. ストリーム暗号の MULTI-S01 と疑似乱数生成器 MUGI の I/O は 7 章と 8 章に示すが, 表 1.3 のインタフェースをほぼ踏襲している

次章以下, 各暗アルゴリズムを示した後, ハードウェアのデータパス構成とタイミングチャートの説明を行う.

表 1.3 ブロック暗号の I/O ポート

ポート名	方向	サイズ	説 明
RSTn	In	1	リセット信号. RSTn=0 で, シーケンサと内部レジスタがリセットされる. リセットは全ての処理に優先し, クロック信号 CLK が入っている限り EN=0 でも, 実行される.
CLK	In	1	システムクロック信号. 全てのレジスタはこのクロックの立ち上がりに同期して, データの入出力を行う.
Kin	In	128	鍵入力ポート.
Din	In	128	データ入力ポート.
Krdy	In	1	EN=1 のとき, Krdy=1 で Kin から秘密鍵を取り込み, 鍵の事前処理が開始される.
Drdy	In	1	EN=1 のとき, Drdy=1 で Din から平文(EncDec=0)または暗号文(EncDec=1)をを取り込み, 直ちに暗号化・復号処理を開始する. Drdy=1 を与える前に鍵の事前処理が完了していなければならない.
EncDec	In	1	EncDec=0 で暗号化, EncDec=1 で復号を行う.
EN	In	1	イネーブル信号. EN=1 でマクロがアクティブとなり, EN=0 のときリセットを除く全ての処理は一時停止する. 再び EN=1 とすると, 一時停止したところから処理が再開する.
Dout	Out	128	データ出力ポート. 暗号化処理の後 Dvld=1 となると暗号文を, 復号処理の場合は平文が出力される. Dvld=1 であるクロックサイクルでのみ有効な値が出力される.
Busy	Out	1	ビジー信号. 鍵の事前処理または暗号化・復号処理が行われている間 Busy=1 となる. Busy=1 の間は, Krdy=1 や Drdy=1 を与えることはできない.
Dvld	Out	1	暗号化または復号処理が終了し, ポート Dout にデータが出力される 1 クロックサイクルの間 Dvld=1 となる.
Kvld	Out	1	リセットまたは鍵が入力された直後に Kvld=0 となり, 鍵の事前処理が終了して鍵レジスタがセットされると, マクロによってその後 Kvld=1 をキープするか, 1 クロックだけ Kvld=1 となる.

2. AES

図 2.1 に 128 ビット鍵による AES アルゴリズムの暗号化処理の流れを示す．入力された秘密鍵は右側の Key Generator によって 11 組のラウンド鍵に変換される．128 ビットの平文データはまず，4 行×4 列の 16 バイトのマトリクス状に並べられ，4 つの基本関数 SubBytes, ShiftRows, MixColumns そして AddRoundKey が繰返し適用される．SubBytes はバイト単位の非線形変換 S-box を 16 個集めたもので，ガロア体 GF(2^8)上の乗法逆元演算に続いてアフィン変換を行なう．復号の InvSubBytes では逆アフィン変換の後に逆元演算が行なわれる． ShiftRows は各 4×4 バイト行列をバイト単位で行ごとに，あらかじめ決められたオフセット分巡回シフトする．復号の逆演算は各行を逆方向にシフトすればよく，これは InvSiftRows と呼ばれる．MixColumns では列方向の 4 バイトを 4 項式の各係数と見なした多項式と乗算を行う．AddRoundKey はビット単位のデータとラウンド鍵との XOR 演算である．鍵スケジューラでは，入力された 128 ビットの秘密鍵 k_0 から 10 組のラウンド鍵 k_1~k_{10} を生成するのに，4 つの S-box(=4 バイト分)と 10 組の 4 バイト定数 rc_1~rc_{10} が用いられる．なお rc_1~rc_{10} の下位 3 バイトは 0 である．復号では鍵が暗号化とは逆の順序で使用されるのと同時に，暗号化の逆関数が暗号文に施されて平文に変換される．

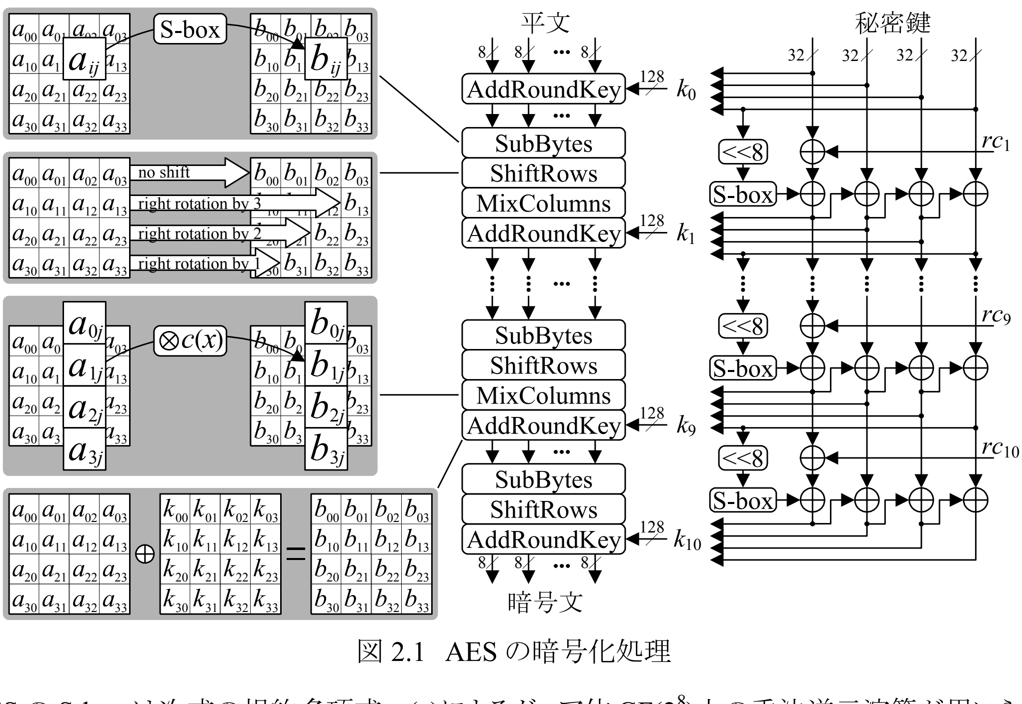


図 2.1 AES の暗号化処理

AES の S-box は次式の規約多項式 $m(x)$によるガロア体 GF(2^8)上の乗法逆元演算が用いられる．

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

暗号化では逆元演算に続いてアフィン変換 A が，復号では逆変換 A^{-1} に続いて逆元演算が行なわれる．

$$A: \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$A^{-1}: \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 \oplus 1 \\ a_1 \oplus 1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \oplus 1 \\ a_6 \oplus 1 \\ a_7 \end{pmatrix}$$

拡散層 MixColumns は 4×4 バイト行列の各列を x の 3 次多項式の 4 つの係数として扱い，次式と乗算じた後に x^4+1 の剰余を求める演算である.

$$c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

復号におけるInvMixColumnsは次の多項式を用いる.

$$c^{-1}(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$$

図 2.2 は高速実装を目的に，内部バス幅を 128 ビットと広く取った AES のデータパスである．S-box 内のガロア体 GF(2^8)の逆元演算器（テーブルで実装）や，マトリクス乗算である MixColumns と InvMixColumns の共通項の共有化を行っている．コンポーネント共有のため，復号で AddRoundKey と InvMixColumns（図 2.2 では InvMixCol.と表示）の順番を入れ替え，かつそのつじつまを合わせるために右半分の鍵スケジューラのラウンド鍵出力に MixColumns を施している.

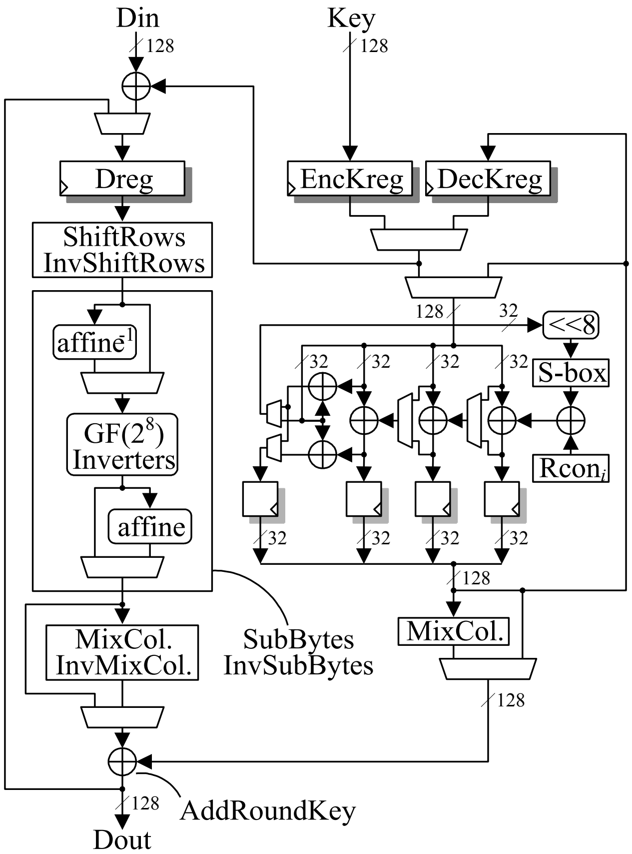


図 2.2 AES 回路のデータパス

図 2.3 に最短サイクルでの暗号化処理のタイミングチャートを示す．各クロックの動作は下記の通りである．

CLK1: RSTn=0 とすることで，制御回路がリセットされる．

CLK2: Krdy=1 とすることで，Kin に入力された 128bit の秘密鍵が内部レジスタにセットされる．

CLK3: EncDec=0 なので暗号化処理であるが，復号処理ブロック側で復号処理の最初のラウンド鍵（暗号化処理の最終ラウンド鍵）を生成する初期化が開始され，ビジー信号 BSY=1 となる．Kout には暗号化処理側の回路ブロックからの出力が接続されているので，鍵初期化時にラウンド鍵は出力されない．

CLK14: 鍵の初期化が終了し，BSY=0，また 1 クロックだけ Kvld=1 となる．それと同時に Din に入力された 128bit の平文が内部レジスタにセットされる．

CLK15: EncDec＝0 なので暗号化処理が開始され，ビジー信号 BSY=1 となる．これから毎クロック，Kout にラウンド鍵が出力されていく．

CLK16~25: 暗号化処理は 0 クロックを要し，CLK25 で完了する．128bit の暗号文が Dout から出力され，BSY=0，データ出力信号 Dvld=1 が 1 クロックだけ出力される．

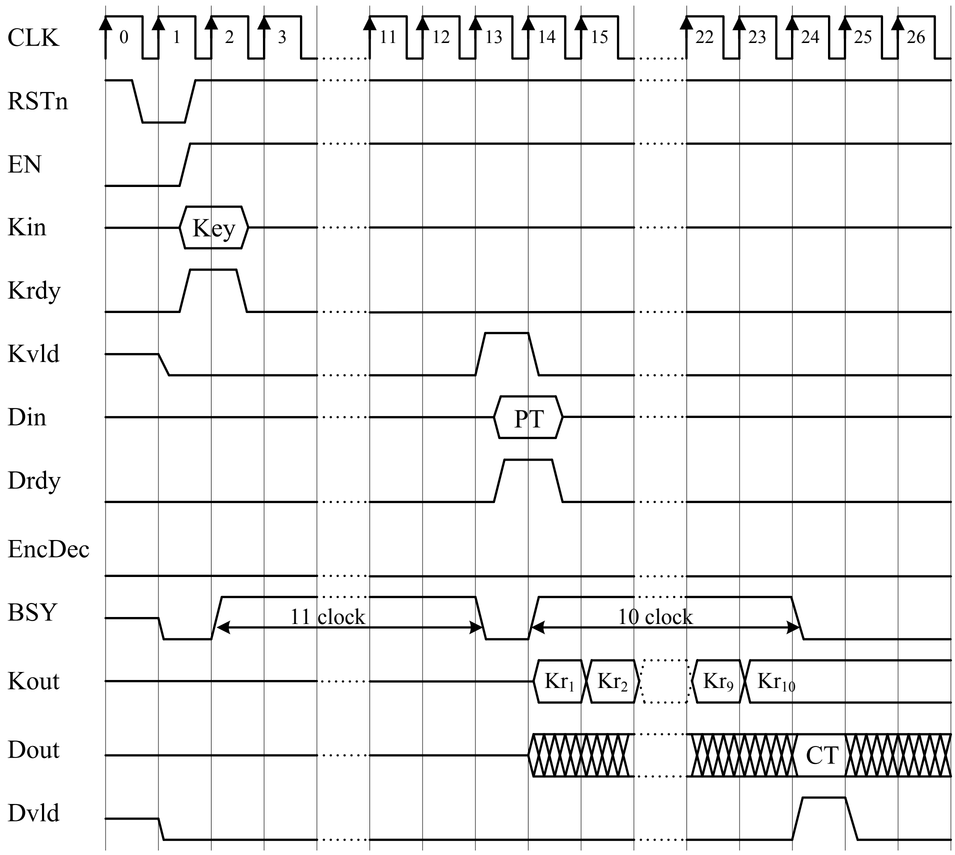


図 2.3 AES の暗号化処理のタイミングチャート

図 2.4 に最短サイクルでの復号処理のタイミングチャートを示す．各クロックの動作は下記の通りである．

CLK1: RSTn=0 とすることで，制御回路がリセットされる．

CLK2: Krdy=1 とすることで，Kin に入力された 128bit の秘密鍵が内部レジスタにセットされる．

CLK3: 復号処理の最初のラウンド鍵(暗号化処理の最終ラウンド鍵)を生成する初期化が開始され，ビジー信号 BSY=1 となる．

CLK14: 鍵の初期化が終了し，BSY=0，また Kvld=1 となる．それと同時に Din に入力された 128bit の暗号文が内部レジスタにセットされる．

CLK15: EncDec＝1 なので復号処理が開始され，ビジー信号 BSY=1 となる．これから毎クロック，Kout にラウンド鍵が出力されていく．

CLK16~25: 復号処理は暗号化処理と同様に 10 クロックを要し，CLK25 で完了する．128bit の平文が Dout から出力され，BSY=0，データ出力信号 Dvld=1 が 1 クロックだけ出力される．

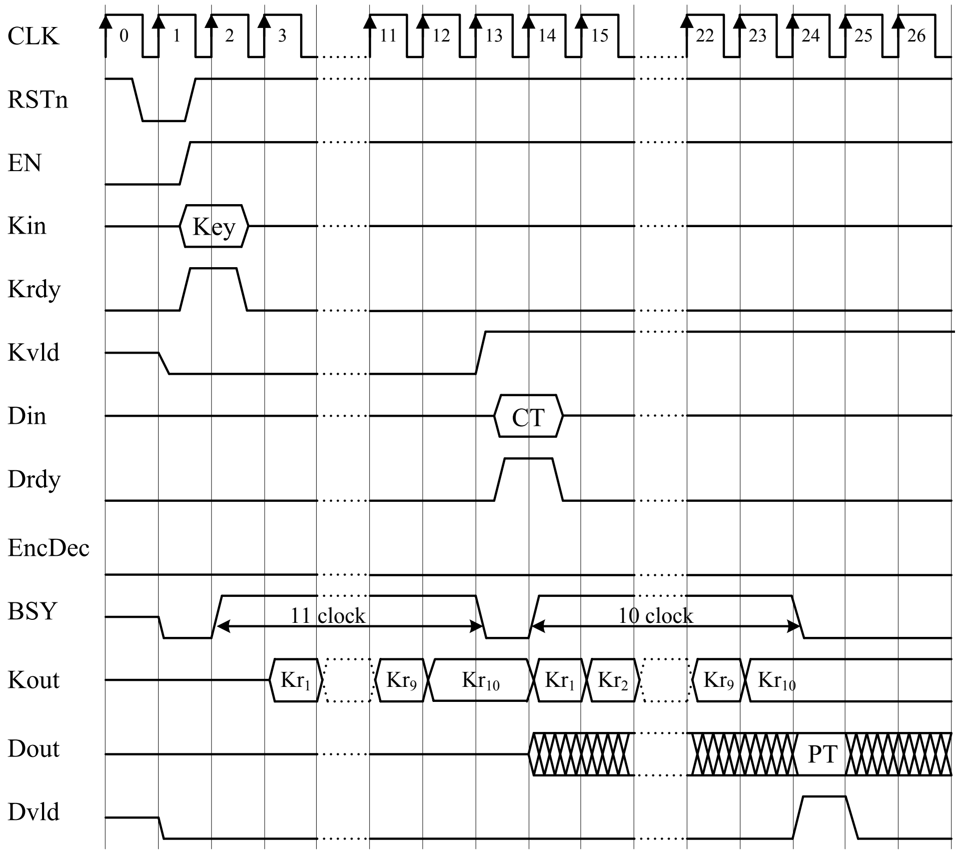


図 2.4 AES の復号処理のタイミングチャート

3. Camellia

図3.1に128ビット鍵によるCamelliaアルゴリズムの暗号化処理を示す．図左半分の22ラウンドのデータ攪拌部は，6ラウンドのFeistelネットワークブロックと，そのブロック間の2つの線形変換FL/FL^{-1}，そして入出力時の128ビットデータと128ビットラウンド鍵とのXORから構成される．128ビットの入力データは，左右64ビットずつに分解され，Feistelネットワークブロックではその左半分がF関数で64ビットラウンド鍵を用いて変換された後，右半分にXORされる．そして左右が入れ替えられて，ラウンド鍵を変えながら同様の処理が繰り返される．F関数への64ビット入力は，64ビットのラウンド鍵とXORされた後，8つの8ビットブロックに分割され，4種類(S1~S4)×2組のS-boxで変換され，さらに64ビット全体に対してP関数による変換が施される．復号は暗号化と同じ処理に対して，ラウンド鍵を逆順にスケジュールすることで実行される．

各ラウンド鍵は128ビットの秘密鍵K_Lと128ビットの中間鍵K_Aを表10のように巡回シフトしたもので，中間鍵K_Aは図3.2に示したように，秘密鍵K_LにF関数を4回施すことで生成される．

表 3.1　鍵スケジューリング

Initial XOR		$kw_{1(64)}$	$(K_L<<<0)_{L(64)}$
		$kw_{2(64)}$	$(K_L<<<0)_{R(64)}$
F	Round 1	$k_{1(64)}$	$(K_A<<<0)_{L(64)}$
	Round 2	$k_{2(64)}$	$(K_A<<<0)_{R(64)}$
	Round 3	$k_{3(64)}$	$(K_L<<<15)_{L(64)}$
	Round 4	$k_{4(64)}$	$(K_L<<<15)_{R(64)}$
	Round 5	$k_{5(64)}$	$(K_A<<<15)_{L(64)}$
	Round 6	$k_{6(64)}$	$(K_A<<<15)_{R(64)}$
FL		$kl_{1(64)}$	$(K_A<<<30)_{L(64)}$
FL^{-1}		$kl_{2(64)}$	$(K_A<<<30)_{R(64)}$
F	Round 7	$k_{7(64)}$	$(K_L<<<45)_{L(64)}$
	Round 8	$k_{8(64)}$	$(K_L<<<45)_{R(64)}$
	Round 9	$k_{9(64)}$	$(K_A<<<45)_{L(64)}$
	Round 10	$k_{10(64)}$	$(K_L<<<60)_{R(64)}$
	Round 11	$k_{11(64)}$	$(K_A<<<60)_{L(64)}$
	Round 12	$k_{12(64)}$	$(K_A<<<60)_{R(64)}$
FL		$kl_{3(64)}$	$(K_L<<<77)_{L(64)}$
FL^{-1}		$kl_{4(64)}$	$(K_L<<<77)_{R(64)}$
F	Round 13	$k_{13(64)}$	$(K_L<<<94)_{L(64)}$
	Round 14	$k_{14(64)}$	$(K_L<<<94)_{R(64)}$
	Round 15	$k_{15(64)}$	$(K_A<<<94)_{L(64)}$
	Round 16	$k_{16(64)}$	$(K_A<<<94)_{R(64)}$
	Round 17	$k_{17(64)}$	$(K_L<<<111)_{L(64)}$
	Round 18	$k_{18(64)}$	$(K_L<<<111)_{R(64)}$
Final XOR		$Kw_{3(64)}$	$(K_A<<<111)_{L(64)}$
		$Kw_{4(64)}$	$(K_A<<<111)_{R(64)}$

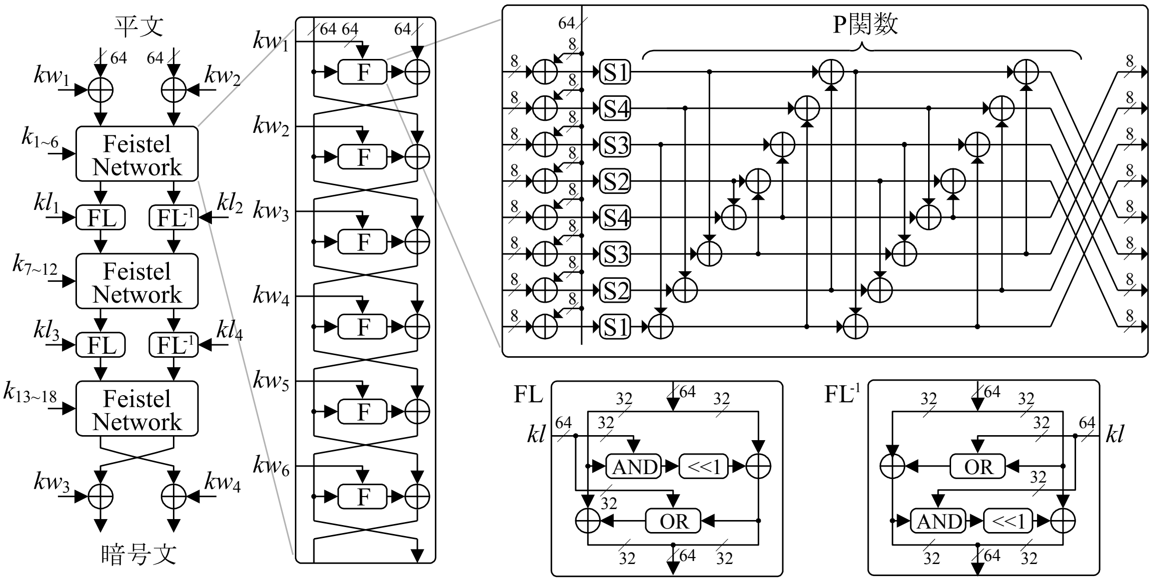


図 3.1 Camellia の暗号化処理

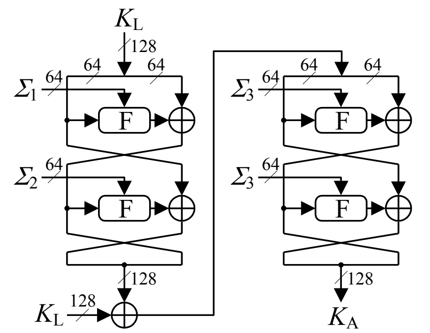


図 3.2 中間鍵 K_A の生成

Camellia の 4 種類の S-box S1~S4 はいずれも，次のガロア体 $GF((2^4)^2)$上の乗法逆元演算と，その前後に施されるアフィン変換 F および H によって構成される．図 3.3 に示したように S1 の出力ビット列を 1 ビット右に巡回シフトした変換が S2，1ビット左巡回シフトしたものが S3，そして入力ビット列を 1 ビット左巡回シフトしたものが S4 である．なお，今回の回路実装では，S-box は 8 ビット入出力のルックアップテーブル実装としている．

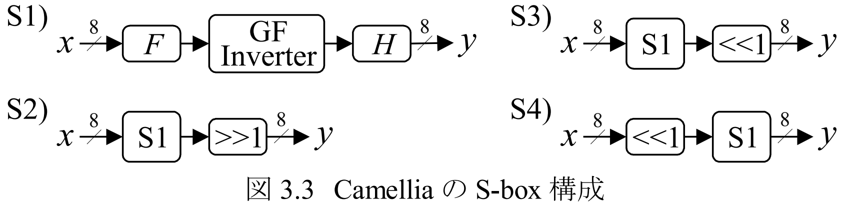


図 3.3 Camellia の S-box 構成

$$\begin{cases} \mathrm{GF}(2^4): & g_0(x)=x^4+x+1 \\ \mathrm{GF}((2^4)^2): & g_1(x)=x^2+x+\omega \quad (\omega=\{1001\}) \end{cases}$$

$$F:\begin{pmatrix}b_0\\b_1\\b_2\\b_3\\b_4\\b_5\\b_6\\b_7\end{pmatrix}=\begin{pmatrix}0&1&0&0&0&1&0&0\\1&0&0&0&0&0&1&0\\0&0&1&0&1&0&0&1\\0&0&1&0&0&0&0&1\\0&0&0&1&0&0&1&0\\0&1&0&0&1&0&0&0\\1&0&0&0&0&0&0&1\\0&0&0&1&0&1&0&0\end{pmatrix}\begin{pmatrix}a_0\oplus 1\\a_1\oplus 1\\a_2\\a_3\\a_4\\a_5\oplus 1\\a_6\\a_7\oplus 1\end{pmatrix}$$

$$H:\begin{pmatrix}b_0\\b_1\\b_2\\b_3\\b_4\\b_5\\b_6\\b_7\end{pmatrix}=\begin{pmatrix}0&1&0&0&1&1&0&0\\0&1&0&0&0&1&0&0\\0&0&0&1&0&0&1&0\\0&1&0&0&0&0&0&1\\0&0&1&0&0&0&1&0\\1&0&0&0&0&0&0&1\\1&0&0&0&1&0&0&0\\0&0&1&0&0&1&0&0\end{pmatrix}\begin{pmatrix}a_0\\a_1\\a_2\\a_3\\a_4\\a_5\\a_6\\a_7\end{pmatrix}\oplus\begin{pmatrix}0\\1\\1\\0\\1\\1\\1\\0\end{pmatrix}$$

図 3.4 に Camellia ハードウェアマクロのデータパスアーキテクチャを示す．1 クロックで変換されるデータビット数は， FL/FL^{-1}, key whitening が 128 ビットで，それ以外は 64 ビットである．1 回の暗号化および復号の処理クロック数は，Key whitening と FL/FL^{-1} に各 2 クロック，F 関数に 18 クロック，データ I/O に 1 クロックで，計 23 クロックとなる．

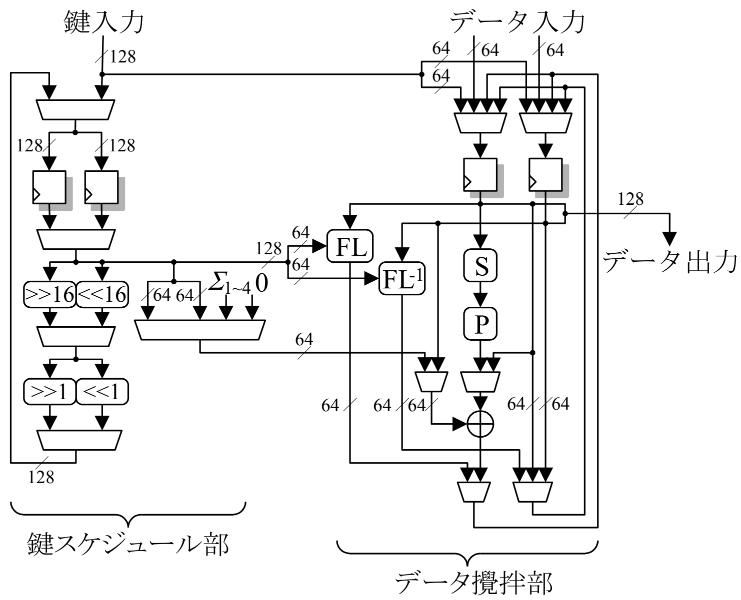


図 3.4 Camellia 回路のデータパス

図 15 は Key whitening の鍵加算の XOR を FL/FL^{-1} 関数と共有化した回路である．単純な鍵加算として XOR を使用するときに邪魔となる，FL/FL^{-1} 関数の巡回シフトをキャンセルするために逆巡回シフトを加えている．

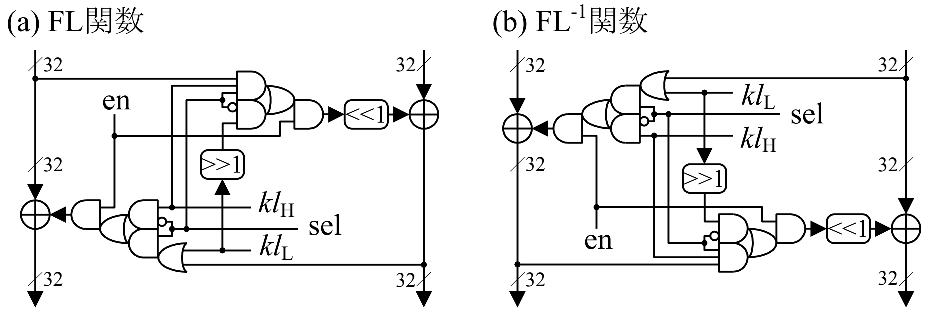


図 3.5　FL/FL^{-1} 回路ブロック

図3.6に暗号化と復号処理のタイミングチャート示す．データ入出力は全てクロックの立ち上がりに同期しており，この例で信号の制御は最短のサイクルで行われている．

CLK1:　リセット信号 RSTn=0 とすることで，シーケンサーロジックと内部レジスタがクリアされる．

CLK2:　イネーブル信号 EN=1，鍵入力用信号 Drdy=1 とすることで，鍵入力ポート Kin 上の秘密鍵 K がマクロの内部鍵レジスタにストアされる．直ちに中間鍵生成処理が開始され，ビジー信号が Busy=1 となる．なお，EncDec=1 なので復号モードとなっているが，鍵設定時にこの信号は影響しない．

CLK7:　中間鍵生成が終了し，鍵が有効となったことを示すステータス信号が Kvld=1 となると同時に Busy=0 に落ちる．

CLK8: Drdy=1 とすることで，EncDec=1(復号モード)となっているため，Din 上のデータ CT が暗号文としてマクロ内のデータレジスタに取り込まれる．それに伴い，復号処理が開始されて Busy=1 となる．

CLK30:　復号処理が終了し Busy=0 に落ち，Dvld=1 となり，データ出力ポート Dout に平文 PT が出力される．

CLK31:　復号処理直後に EncDec=0 として暗号化モードに切り替え，Drdy=1 として平文 PT を取り込む．これにより直ちに暗号化処理が開始されて Busy=1 となり，Dout 上のデータは無効となる．

CLK53:　暗号化処理が終了し Busy=0 に落ち，Dout に有効な暗号文 CT が出力され，Dvld=1 となる．この時点で既に EncDec=1 として復号モードが選択されているが，この信号はデータ入力時にのみ参照されるため，処理途中の変更は無視されている．

CLK54:　EncDec=1(復号モード)となっているので，Drdy=1 により，Din 上のデータが暗号文として取り込まれ，復号処理が始まり Busy=1 となる．前のクロックで出力された暗号文は無効となり，Dvld=0 に落ちる．

CLK76:　復号が終了し Busy=0 に落ち，Dout に平文 PT が出力されて Dvld=1 となる．

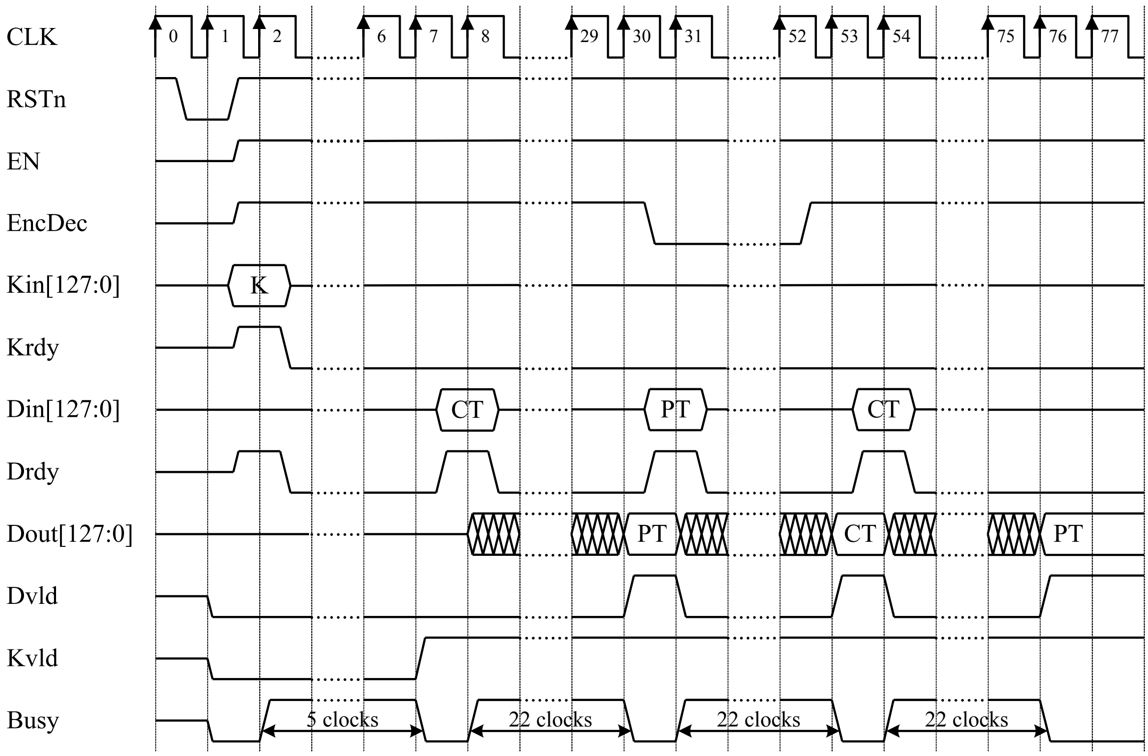


図 3.6 暗号化･復号処理のタイミングチャート

4. CIPHERUNICORN-A

図4.1に128ビット鍵によるCIPHERUNICORN-Aアルゴリズムの暗号化・復号の処理を示す．入力データは初期処理として拡大鍵加算された後，16段Feistel構造により撹拌され，終期処理として拡大鍵減算を行い，処理結果が出力される．図4.2に示すF関数ブロックはテーブル実装によるバイト単位での非線形変換とXORを中心に構成される．図4.3に示す128ビット鍵の鍵スケジューラでは，初期処理，終期処理，ラウンド処理用の拡大鍵を生成する．12 段のMT関数に続き，16段のMT関数の循環処理毎に8個の32ビット拡大鍵が生成され，9回の繰り返しで72個の32ビット拡大鍵が得られる．これらの拡大鍵はラウンド処理の順に生成されないため on-the-fly による鍵生成を行うことはできず，拡大鍵は鍵メモリにストアされる．

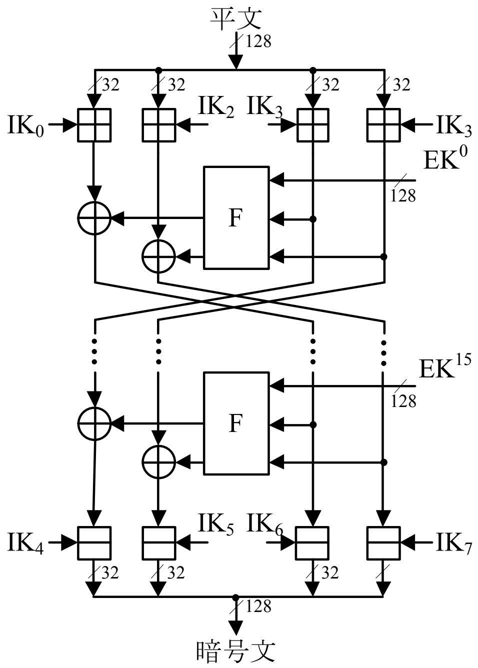


図 4.1 CIPHERUNICORN-A の暗号化処理

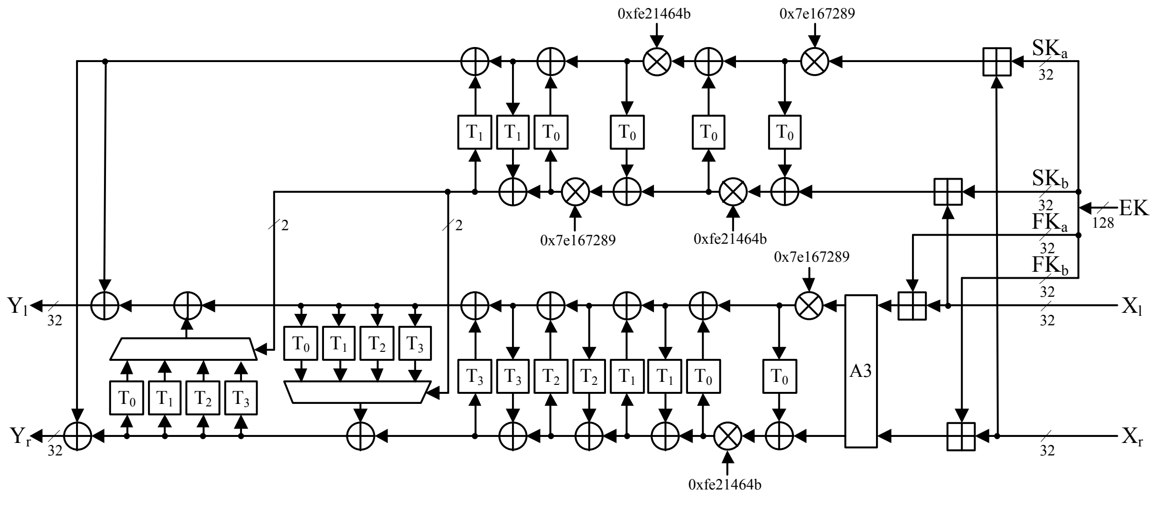


図 4.2 CIPHERUNICORN-A のランダム化関数 F

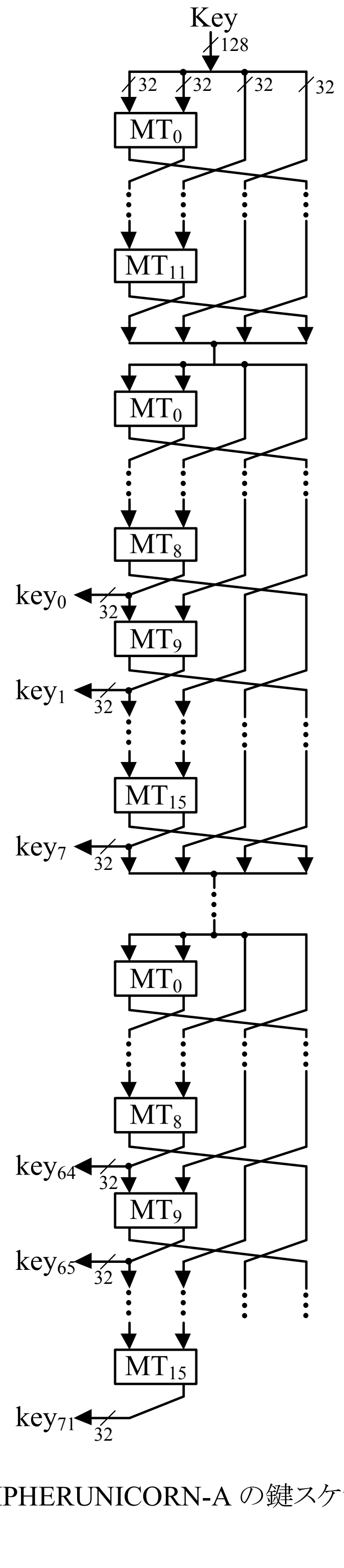


図 4.3 CIPHERUNICORN-A の鍵スケジューリング

図 4.4~4.6 に CIPHERUNICORN-A 回路マクロのデータパスアーキテクチャを示す．F 関数を中心に 1 クロックで 1 ラウンドを構成し，1 クロックあたり 128 ビットが処理される．1 回の暗号化と復号の処理クロック数は，16 段のラウンド処理に 16 クロック，データ I/O に 1 クロックで,計 17 クロックである．

ラウンド鍵は事前計算により鍵レジスタに保持されており，初期処理と終期処理に各 128 ビット，ラウンド処理毎に 128 ビットの拡大鍵が供給される．

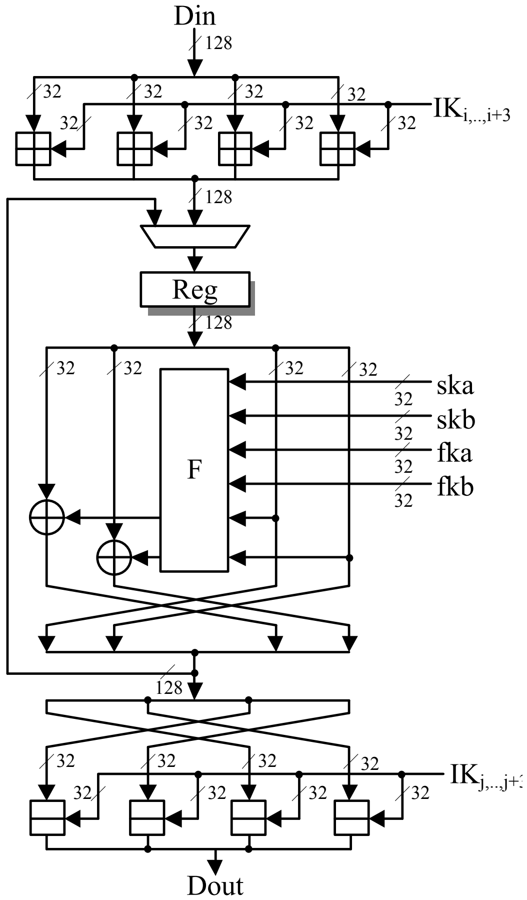


図 4.4　CIPHERUNICORN-A 回路のデータパス

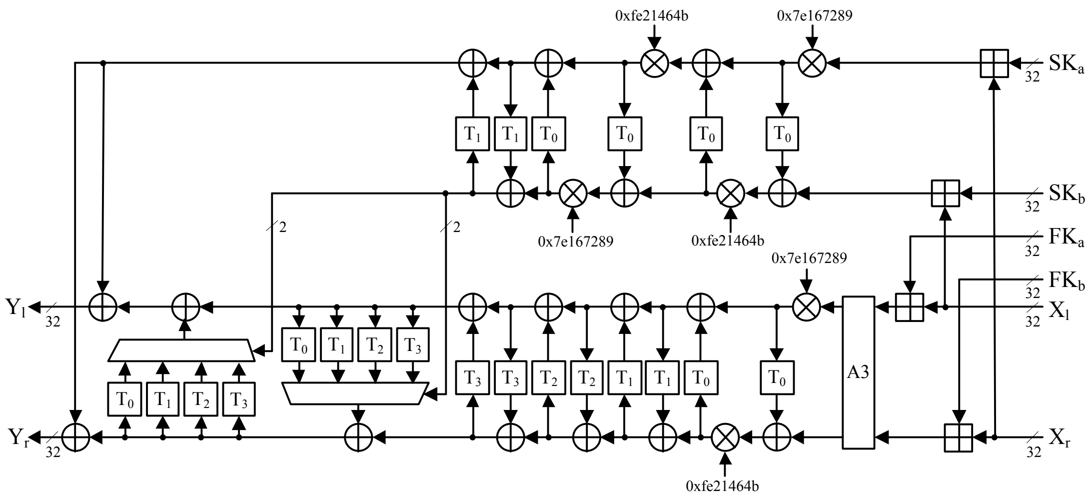


図 4.5　F 関数ブロック

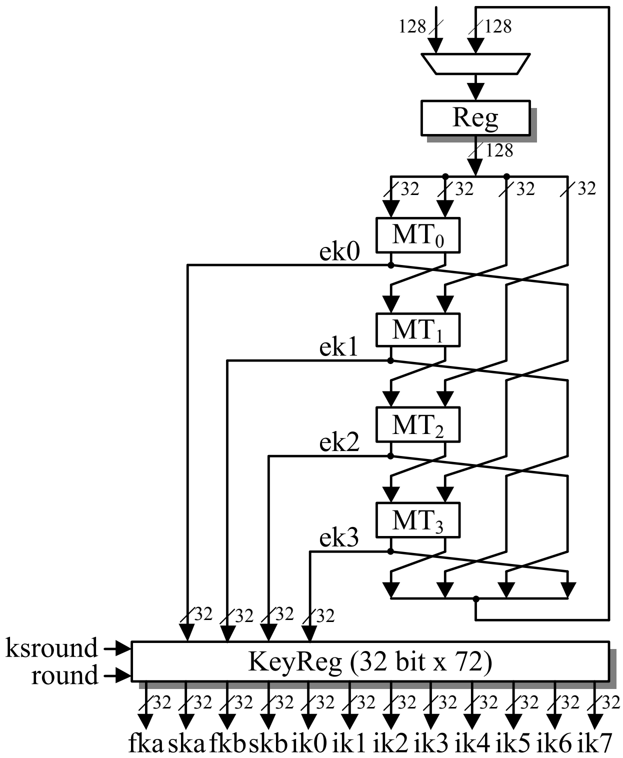


図 4.6　鍵スケジューリング部

F 関数では 128 ビットのラウンドデータのうち，Feistel 構造の半分である 64 ビットのデータとラウンド鍵を入力として処理を行う．A3 関数は図 4.7 のように循環シフトと XOR によって構成される．また T0～T3 関数は図 4.8 のように，8 ビットテーブル S0～S3 で構成される．定数乗算は乗算器を使用せず，シフトと加減算により実装される．

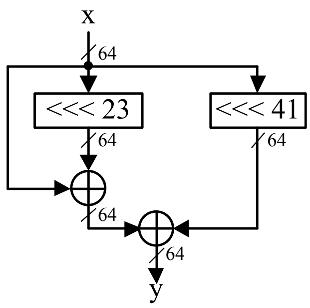


図 4.7　A3 関数ブロック

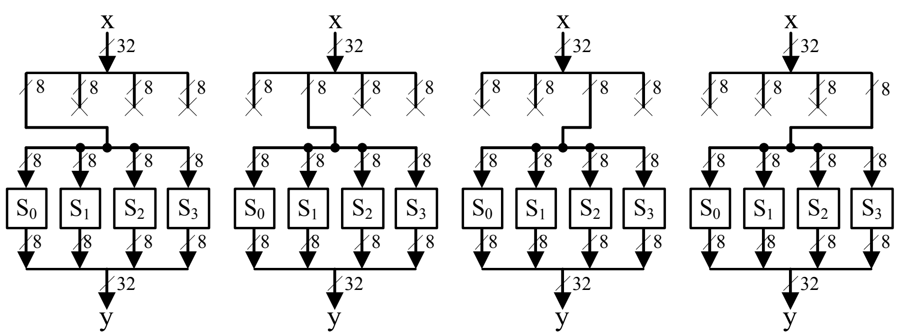


図 4.8　T0 関数・T1 関数・T2 関数・T3 関数ブロック

鍵スケジューリング部は 1 クロックあたり，図 4.9 の MT 関数 4 段で構成され，3 クロック 12 段のダミーループの後，4 クロック 16 段毎に 8 個の 32 ビット拡大鍵が鍵レジスタにストアされ,これを 9 回繰り返すことによって 72 個の拡大鍵が得られる．鍵スケジューリング部による事前鍵生成には，ダミーループ 3 クロック，鍵生成 36 クロック，データ I/O1 クロックの計 40 クロックを要する．MT 関数の定数乗算は乗算器ではなく，シフトと加算回路によって構成される．

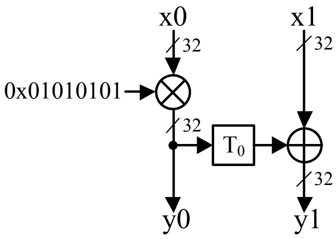


図 4.9 MT 関数ブロック

図 4.10 および図 4.11 にそれぞれ，暗号化と復号処理のタイミングチャート示す．データ入出力は全てクロックの立ち上がりエッジに同期しており，信号の制御は最短のサイクルで行われている．

CLK1: リセット信号 RSTn=0 とすることで，シーケンサーロジックと内部レジスタがクリアされる．

CLK2: イネーブル信号 EN=1，鍵入力用信号 Drdy=1 とすることで，鍵入力ポート Kin 上の秘密鍵 K がマクロの内部鍵レジスタにストアされる．直ちに中間鍵生成処理が開始され，ビジー信号が Busy=1 となる．

CLK41: 中間鍵生成が終了し，鍵が有効となったことを示すステータス信号が Kvld=1 となると同時に Busy=0 に落ちる．

CLK42: Drdy=1，EncDec=0(暗号化モード)であるため，Din 上のデータ PT が平文としてマクロ内のデータレジスタに取り込まれる．それに伴い，暗号化処理が開始され Busy=1 となる．

CLK58: 暗号化処理が終了し Busy=0 に落ち，Dvld=1 となり，データ出力ポート Dout に暗号文 CT が出力される．

CLK59: Drdy=1，EncDec=0(暗号化モード)であるため，Din 上のデータ PT が平文としてマクロ内のデータレジスタに取り込まれる．これにより，次の暗号化処理が開始され,Busy=1 となる．

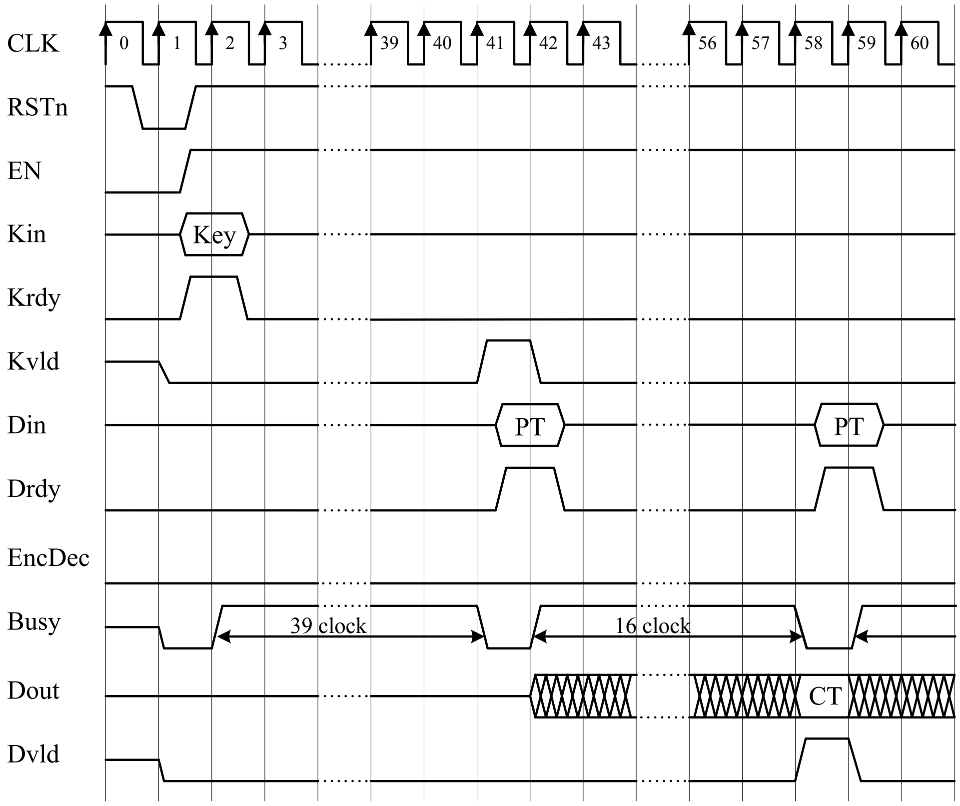


図 4.10　暗号化処理のタイミングチャート

CLK1: リセット信号 RSTn=0 とすることで，シーケンサーロジックと内部レジスタがクリアされる.

CLK2: イネーブル信号 EN=1，鍵入力用信号 Drdy=1 とすることで，鍵入力ポート Kin 上の秘密鍵 K がマクロの内部鍵レジスタにストアされる．直ちに中間鍵生成処理が開始され，ビジー信号が Busy=1 となる.

CLK41: 中間鍵生成が終了し，鍵が有効となったことを示すステータス信号が Kvld=1 となると同時に Busy=0 に落ちる.

CLK42: Drdy=1，EncDec=1(復号モード)であるため，Din 上のデータ CT が暗号文としてマクロ内のデータレジスタに取り込まれる．それに伴い，復号処理が開始されて Busy=1 となる.

CLK58: 復号処理が終了し Busy=0 に落ち，Dvld=1 となり，データ出力ポート Dout に平文 PT が出力される.

CLK59: Drdy=1，EncDec=1(暗号化モード)であるため，Din 上のデータ CT が暗号文としてマクロ内のデータレジスタに取り込まれる．これにより,次の復号処理が開始され,Busy=1 となる.

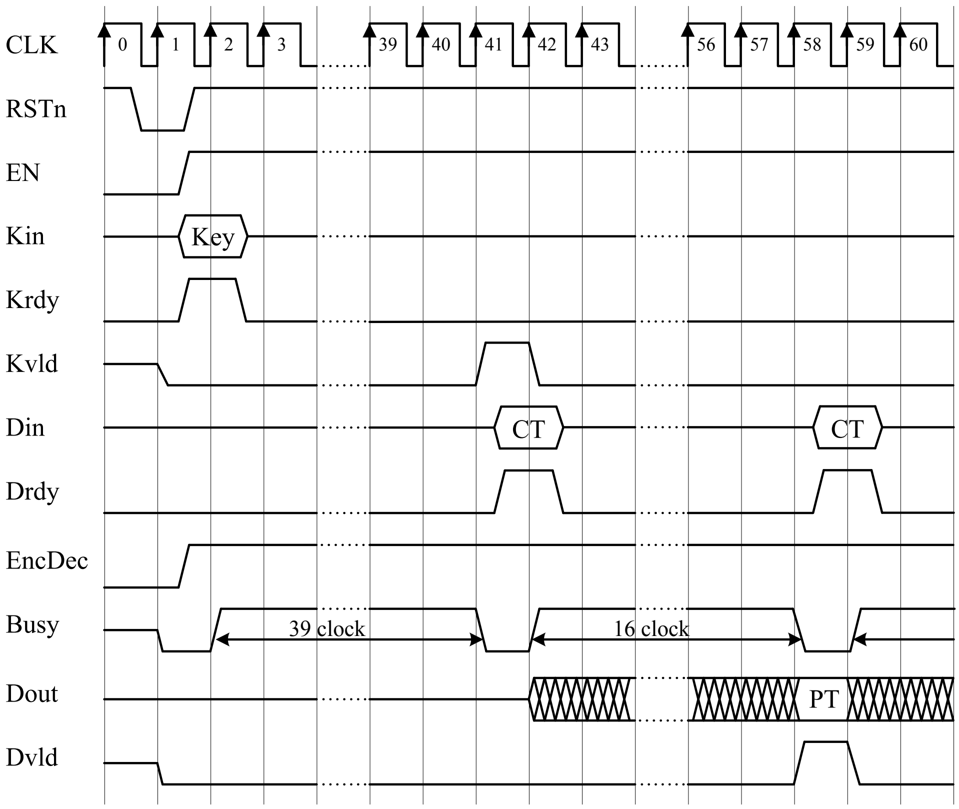


図 4.11　復号処理のタイミングチャート

5. Hierocrypt-3

128 ビット鍵の Hierocrypt-3 の暗号化と復号の処理をそれぞれ図 5.1 と図 5.2 に示す．暗号化は，初期鍵加算 BK，4 段の ρ 関数，1 段の XS 関数と最終鍵加算 AK で構成される．高速なラウンド関数を持つ SPN 構造であるため高速化に向いている反面，拡散層 MDS_L と MDS_H 処理単位が異なるためデータパスの分割による小型化は難しい．Hierocryot-3 の鍵スケジュールは，図 5.3 のように，繰り返し段構造からなる中間鍵生成部と，各中間鍵から拡大鍵を生成する拡大鍵生成部から構成される．

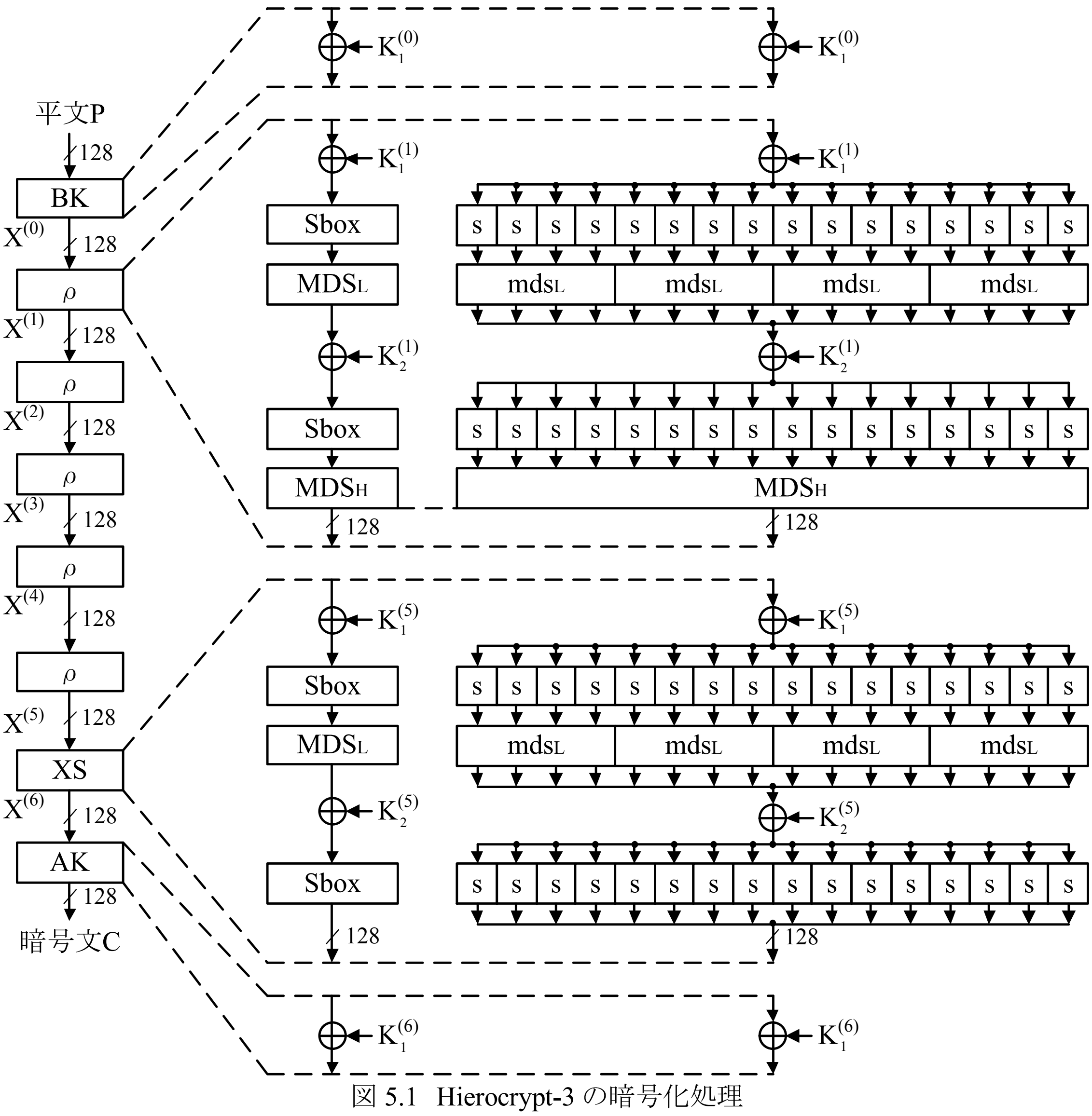


図 5.1 Hierocrypt-3 の暗号化処理

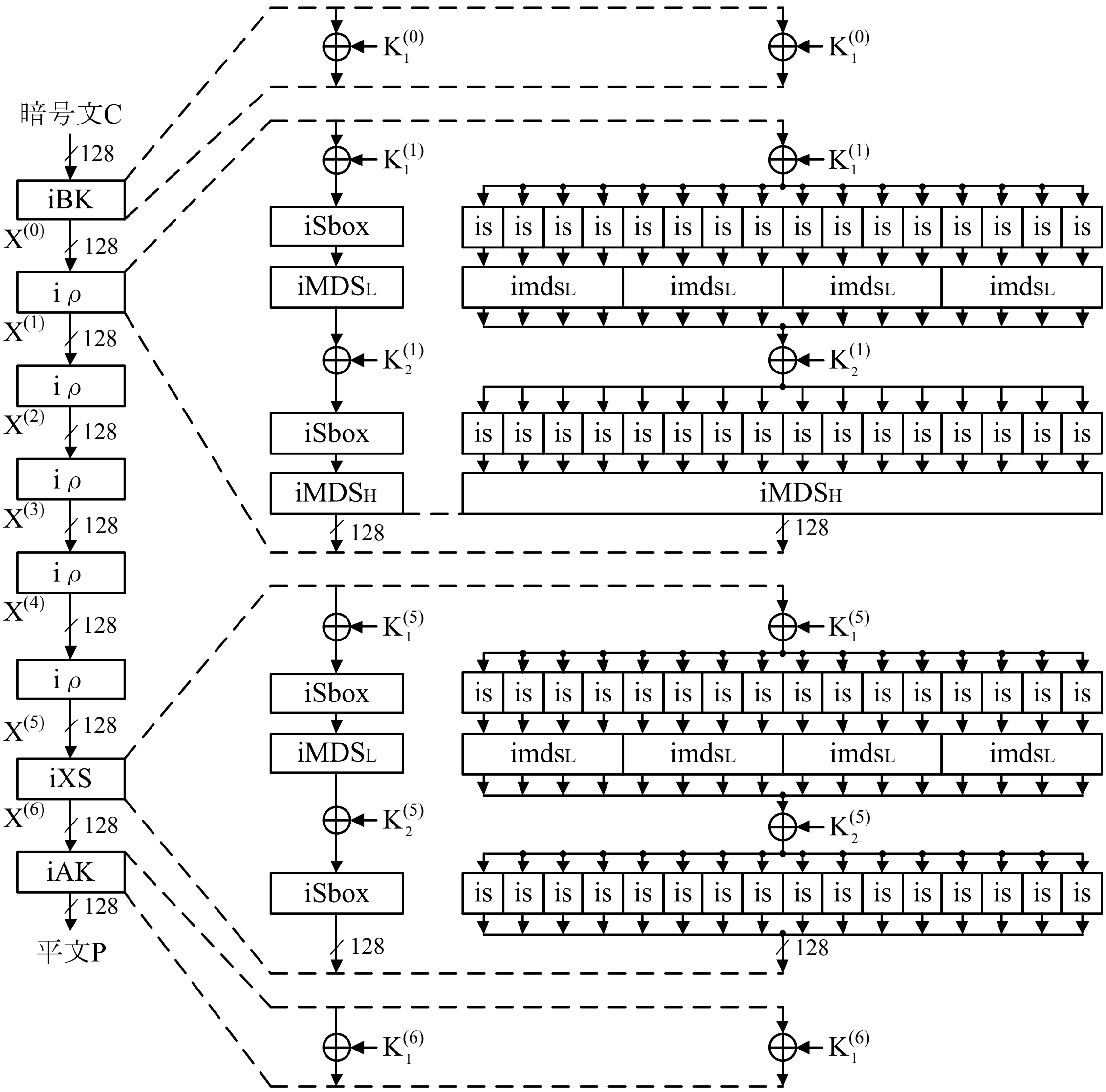


図 5.2　Hierocrypt-3 の復号処理

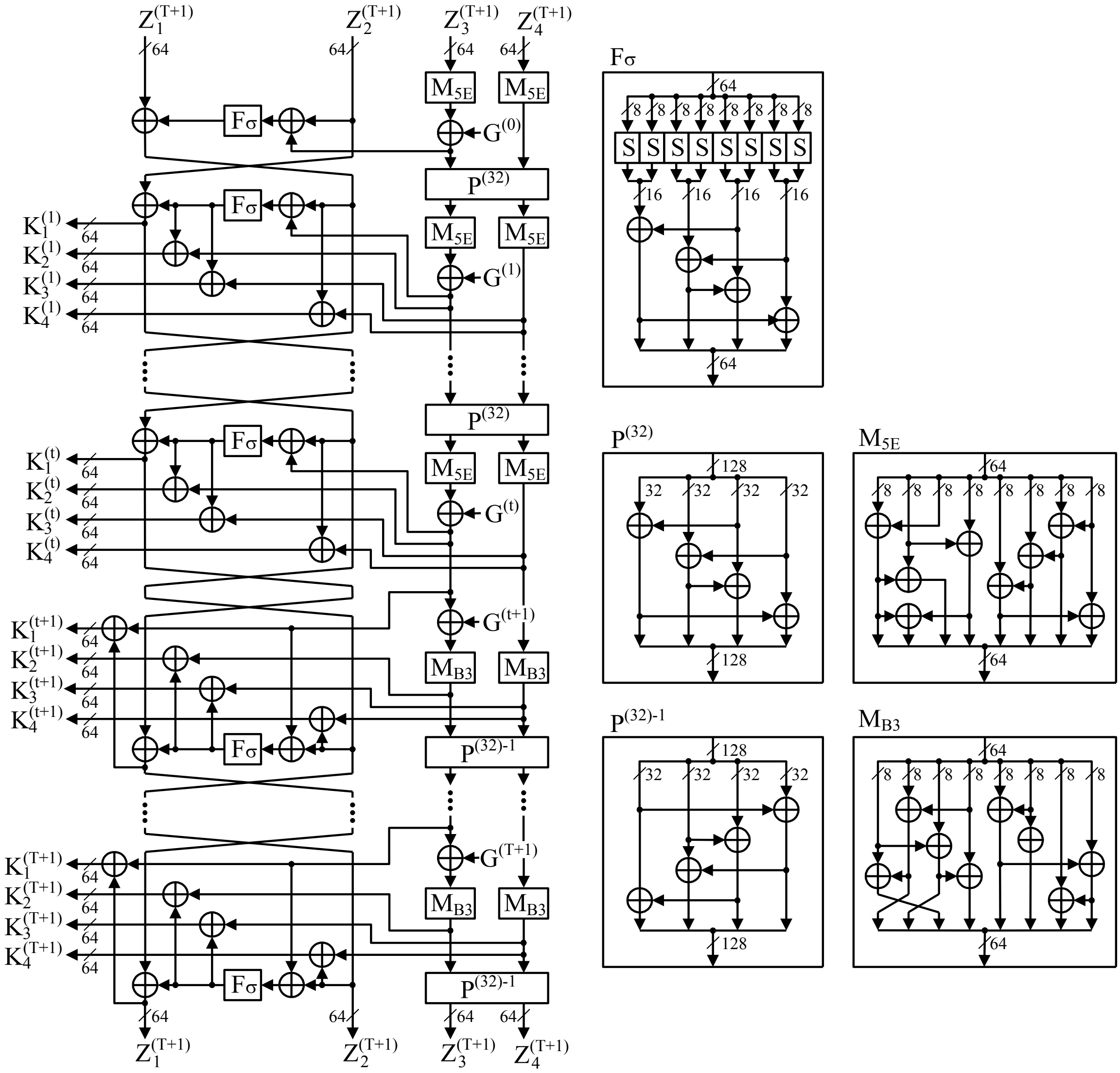


図 5.3 Hierocryot-3 の鍵スケジュール処理

図 5.4 に Hirocrypt-3 ハードウェアマクロの暗号化データパスアーキテクチャを，図 5.5 に復号処理と鍵スケジュールのデータパスアーキテクチャを示す．データパスは基本的に128 ビットとしたが，仕様書通りに組んだところ，ターゲットデバイスの Virtex-5 に実装することができなかったため，多くの関数を 32 ビットや 64 ビットの回路ブロックとし，繰り返し利用することとした．このため，サイクル数が増大している．

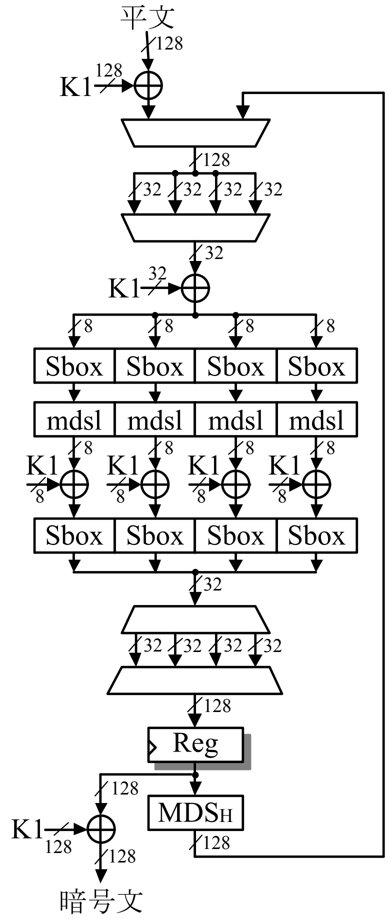


図 5.4 Hierocrypt-3 の暗号化回路のデータパス

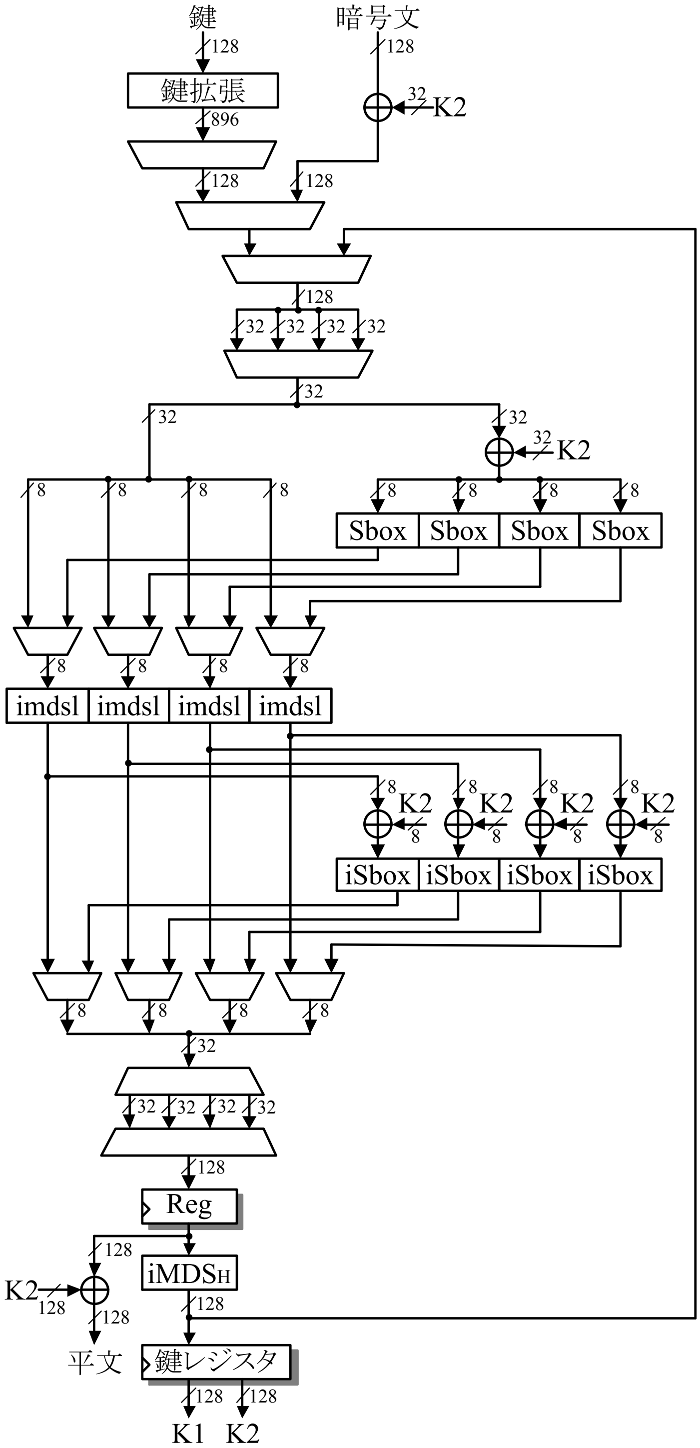


図 5.5　Hierocrypt-3 の復号と鍵スケジュール回路のデータパス

図 5.6 および図 5.7 にそれぞれ，暗号化と復号処理のタイミングチャートを示す．データ入出力は全てクロックの立ち上がりエッジに同期しており，信号の制御は最短のサイクルで行われている．

CLK1：リセット信号 RSTn=0 とすることで，シーケンサーロジックと内部レジスタが初期化される．

CLK2：鍵入力に秘密鍵をセットして，イネーブル信号 EN=1，鍵レディ信号 Krdy=1 とすることで，秘密鍵が取り込まれ鍵生成処理が開始されビジー信号が Busy=1 となる．

CLK888：鍵生成処理が終了したことを示す鍵処理終了信号 Kvld=1 が出力されると同時に，Busy=0 となる．

CLK890：平文 PT をデータ入力ポート Din にセットし，暗号，復号処理選択信号 EncDec=0 と暗号処理モードにしてデータレディ信号 Drdy=1 とすることで暗号化処理が開始される．それと同時に Bus=1 となる．

CLK1377：暗号化処理が終了したことを示すデータ出力信号 Dvld=となり，出力ポート Dout には，暗号文 CT が出力される．また，それと同時に Busy=0 となる．

CLK1379：次の平文が入力可能となる．

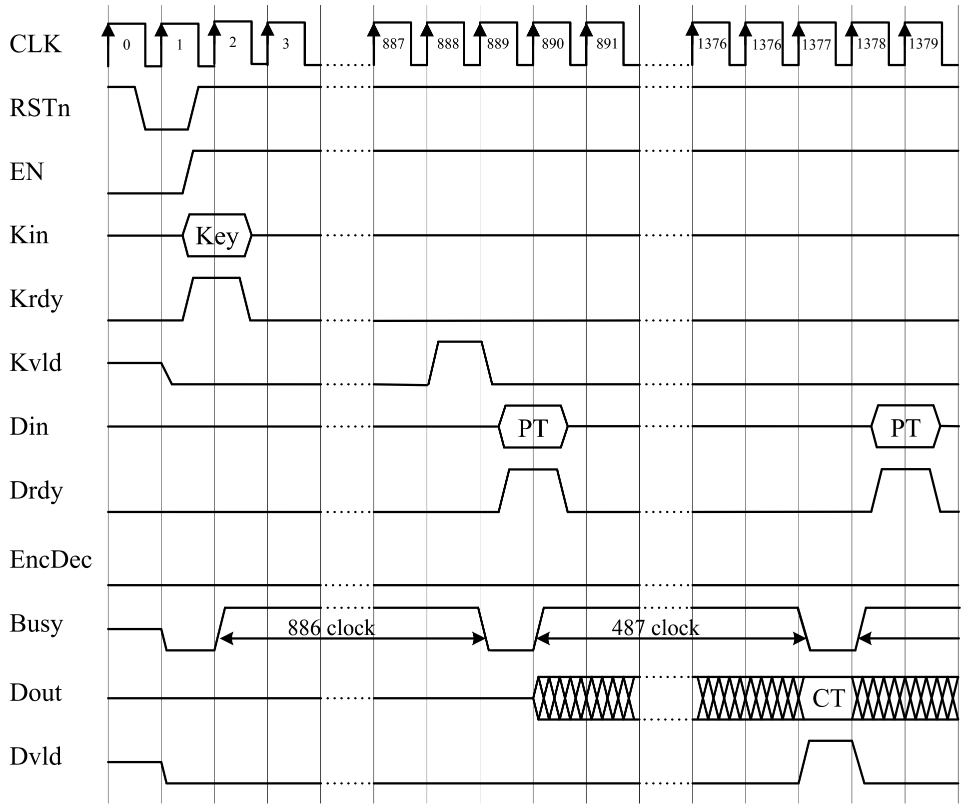


図 5.6 暗号化処理のタイミングチャート

CLK1：リセット信号 RSTn=0 にすることで，シーケンサーロジックと内部レジスタが初期化される．

CLK2：鍵入力に秘密鍵をセットして，イネーブル信号 EN=1，鍵レディ信号 Krdy=1 とすることで，秘密鍵が取り込まれ鍵生成処理が開始される，それと同時にビジー信号 Busy=1 となる．

CLK888：鍵生成処理が終了したことを示す鍵処理終了信号が Kvld=1 に，それと同時に Busy=0

となる.

CLK890：暗号文 CT をデータ入力ポート Din に入力, 暗号化/復号処理選択信号を復号処理の EncDec=1 に, データレディ信号を Drdy=1 とすることで暗号化処理が開始される. それ同時に Busy=1 となる.

CLK1377：復号化処理が終了したことを示すデータ出力信号 Dvld=1 となり, データ出力ポート Dout に平文 PT が出力される. また同時に Busy=0 となる.

CLK1379：次の暗号文が入力可能となる.

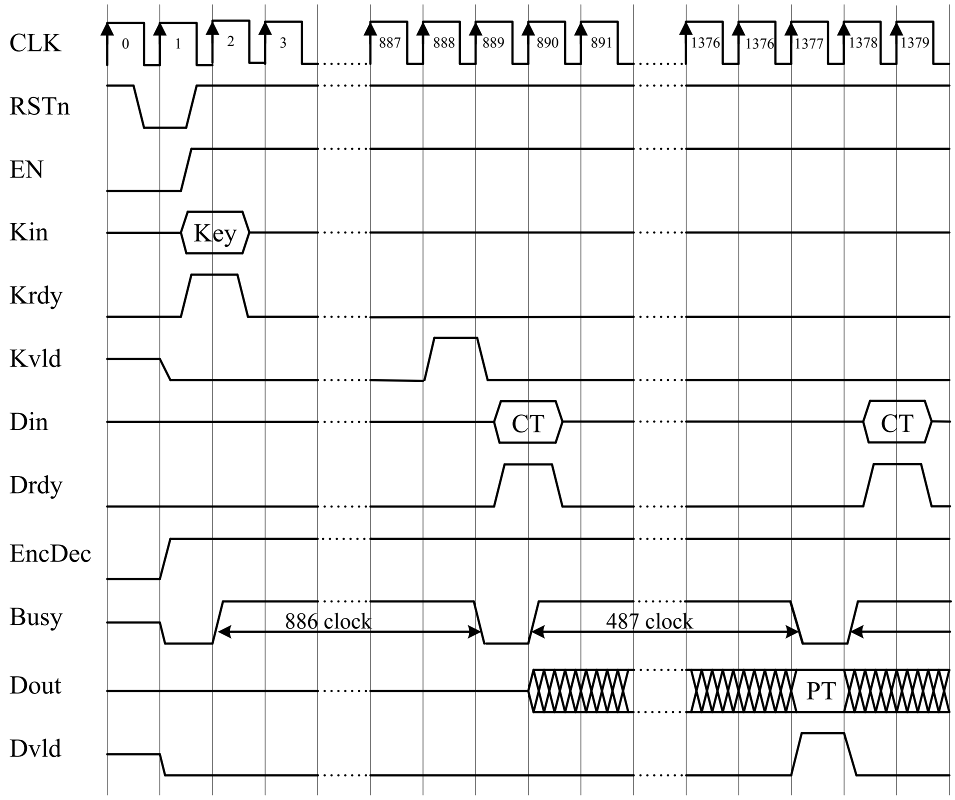


図 5.7 復号処理のタイミングチャート

6. SC2000

図6.1および図6.2に，128ビット鍵によるSC2000アルゴリズムの暗号化と復号の処理を示す．SC2000のデータ攪拌部はFeistel構造とSPN構造が重ね合わされた構造を持ち，鍵をXORするI関数が14段，SPN型攪拌関数であるB関数(復号ではB^{-1}関数)が7段，Feistel型攪拌関数であるR関数が12段の合計33段で構成される．鍵スケジューリング部は，32ビット拡大鍵56個を生成する，中間鍵生成関数と拡大鍵生成関数から構成される．

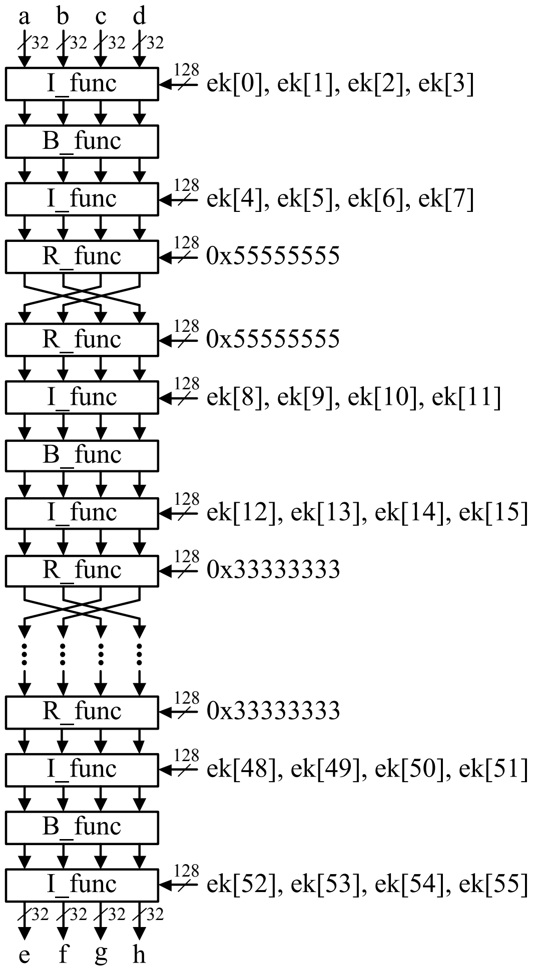


図 6.1 2000 の暗号化処理

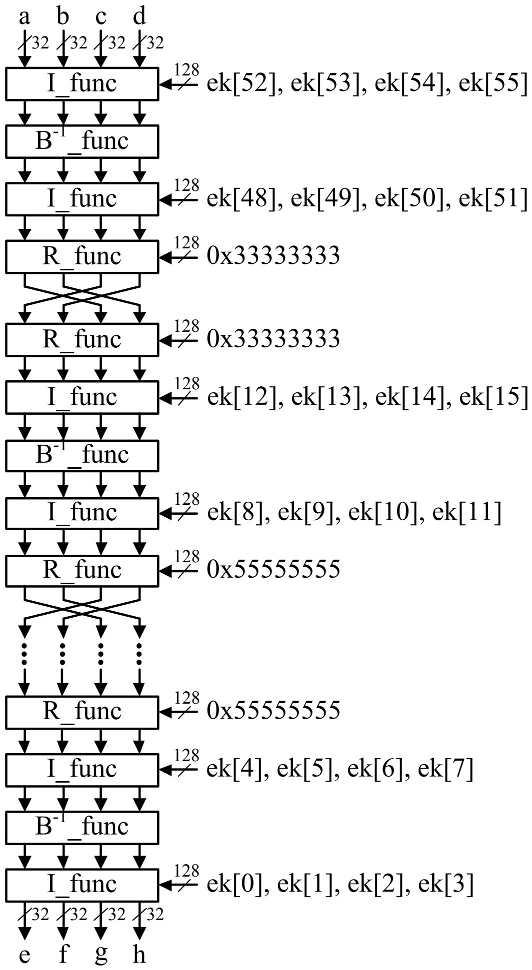


図 6.2 SC2000 の復号処理

図 6.3 および図 6.4 に SC2000 回路ロのデータパスアーキテクチャを示す．I 関数，B(B^{-1})関数，R 関数で構成され，暗号化と復号処理で必要な関数を選択できるようにセレクタを介して接続されている．1 回の暗号化と復号処理のクロック数は，14 段のラウンド処理に 14 クロック，データ I/O に 1 クロックで，計 15 クロックである．ラウンド鍵は事前計算により鍵レジスタに保持されており，1 ラウンドあたり 128 ビットの拡大鍵が供給される．クロックサイクルと，データ攪拌部の構成を表 6.1 に示す．

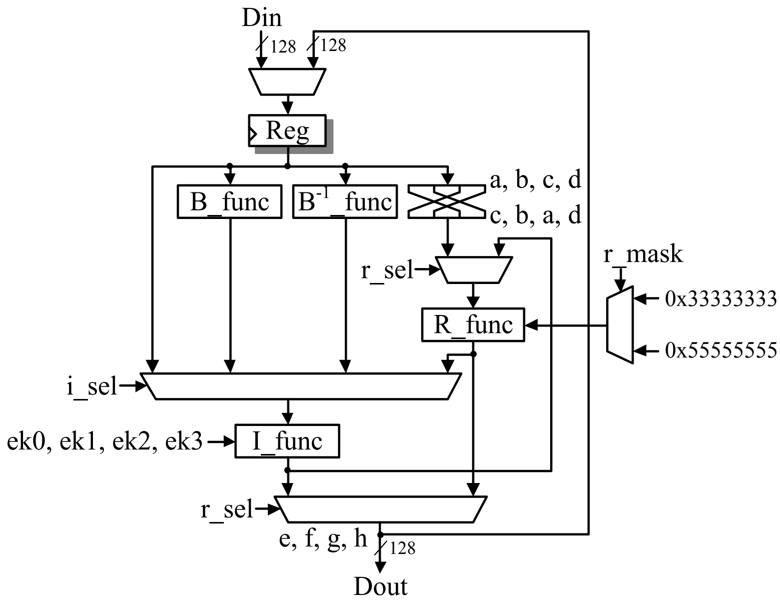


図 6.3 データ攪拌部のデータパス

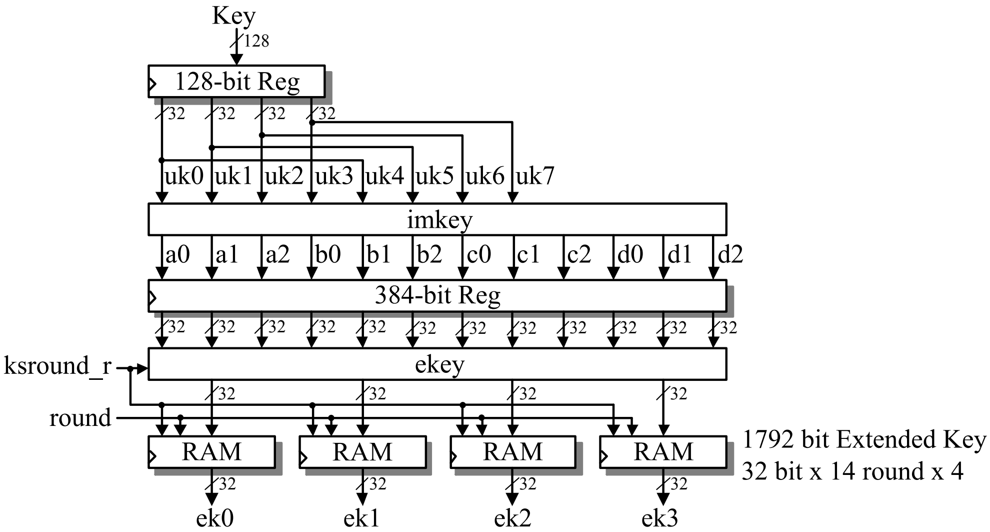


図 6.4 鍵スケジューリング部のデータパス

表 6.1 データ攪拌部の構成

ラウンド	暗号化	復号
1	I	I
2	B, I, R	B^{-1}, I, R
3	R, I	R, I
4	B, I, R	B^{-1}, I, R
5	R, I	R, I
6	B, I, R	B^{-1}, I, R
7	R, I	R, I
8	B, I, R	B^{-1}, I, R
9	R, I	R, I
10	B, I, R	B^{-1}, I, R
11	R, I	R, I
12	B, I, R	B^{-1}, I, R
13	R, I	R, I
14	B, I	B^{-1}, I

図 6.5～図 6.8 に, データ攪拌部の各構成時のデータパスを示す. なお, ラウンド 14 では R 関数ブロックはバイパスされる.

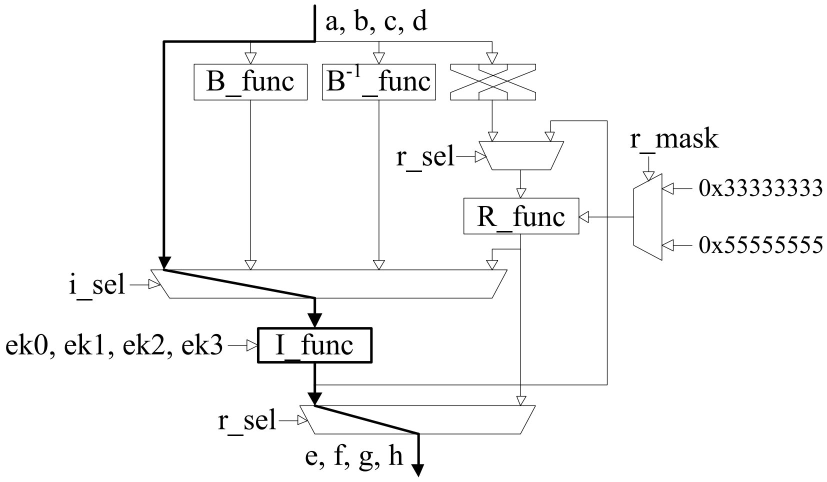


図 6.5　I 関数処理時のパス

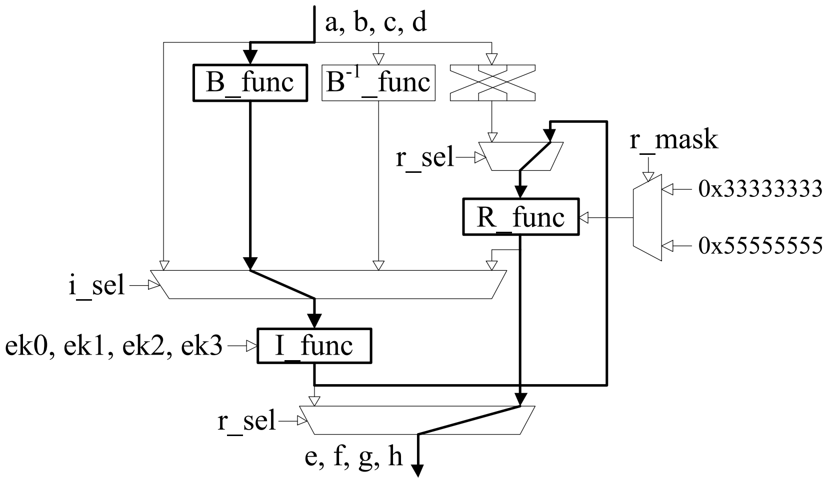


図 6.6　B 関数+I 関数+R 関数処理時のパス

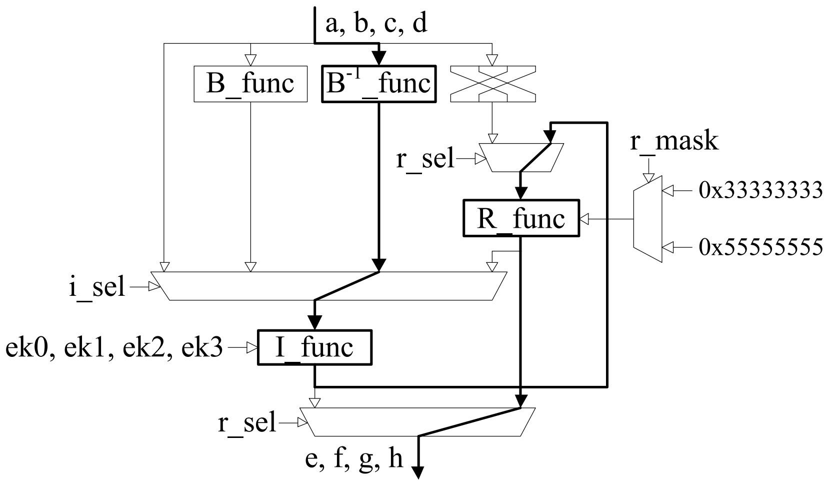


図 6.7　B^{-1} 関数+I 関数+R 関数処理時のパス

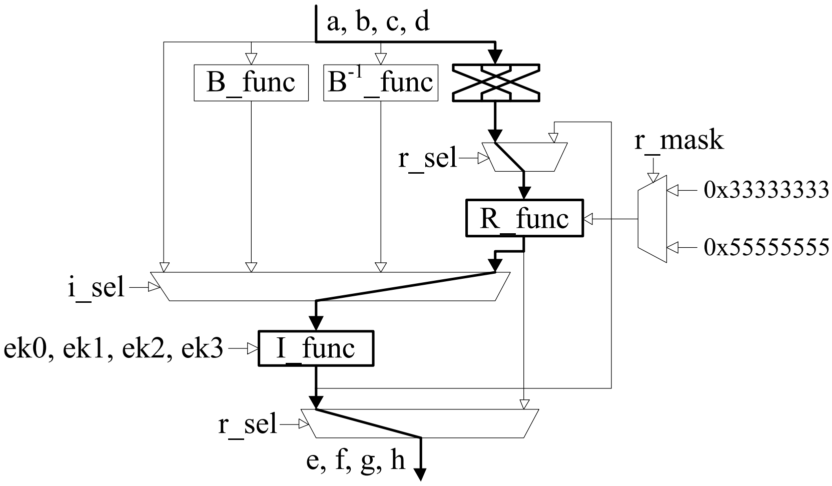


図 6.8 R 関数+I 関数処理時のタパス

I 関数は，図 6.9 のように 128 ビットの入力データと 128 ビットのラウンド鍵の XOR 演算を行う．R 関数は図 6.10 のような Feistel 構造の処理を行うため，128 ビットの入力データのうち，半分の 64 ビットを F 関数で処理して，残り半分の 64 ビットと XOR 演算を行う．また，14 ラウンド用に R 関数をバイパスするためのセレクタを備える．

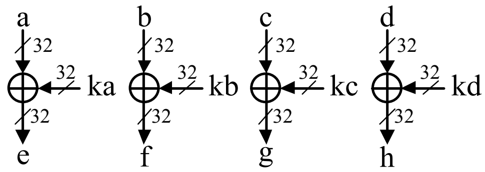


図 6.9 I 関数ブロック

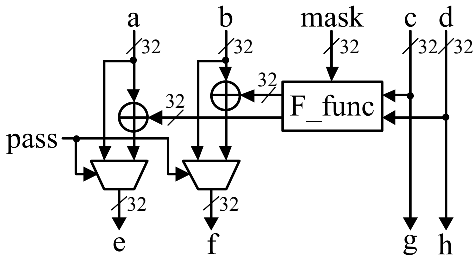


図 6.10 R 関数ブロック

F 関数は，図 6.11 のように 64 ビットの入力データの 32 ビットずつを S 関数と M 関数で処理し，それらを L 関数で処理して出力する．S 関数は 32 ビットの非線形関数で，図 6.12 のように 5 ビットと 6 ビットの S-box から構成され，それぞれをテーブル実装している．M 関数は，図 6.13 のように定数行列の M matrix との行列演算を行う線形関数である．L 関数は図 6.14 のように，ラウンドによって選択される 32 ビットのマスク値との AND 演算と XOR 演算である．

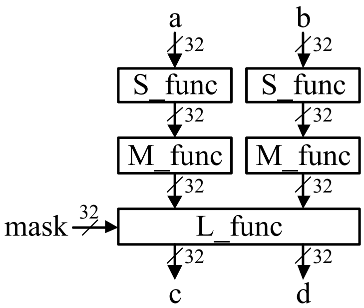


図 6.11 F 関数ブロック

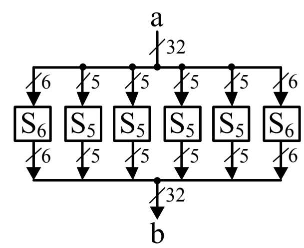


図 6.12 S 関数ブロック

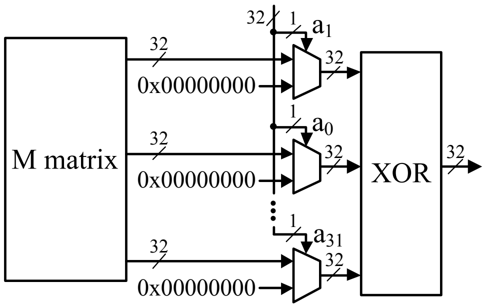


図 6.13 M 関数ブロック

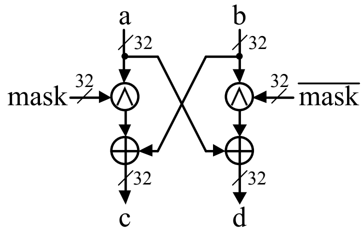


図 6.14 L 関数ブロック

図 6.15 および図 6.16 で，B 関数・B $^{-1}$ 関数を構成する S-box はテーブル実装している．アルゴリズム仕様書上の T 関数と T $^{-1}$ 関数はビット入れ替えであり，これらを独立したモジュールとしては実装していない．

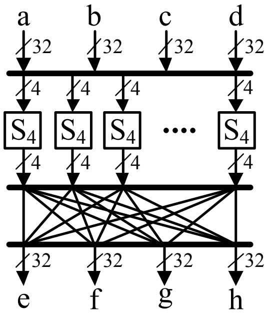


図 6.15 B 関数ブロック

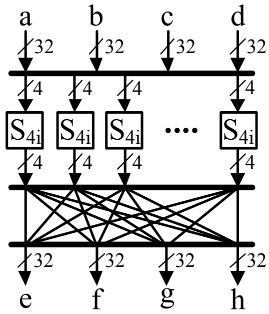


図 6.16 B^{-1} 関数ブロック

図 6.17 に示すように，中間鍵生成関数は 64 ビットの鍵から 32 ビットの中間鍵を計算する図 6.18 の基本モジュール 12 組で構成され，最大 256 ビットの秘密鍵から 384 ビットの中間鍵を生成する．128 ビットの秘密鍵の場合には，{uk0, uk1, uk2, uk3} = {uk4, uk5, uk6, uk7} となる．MS(4i+j)は 32 ビット定数となるため，事前に計算した定数値を用いる．

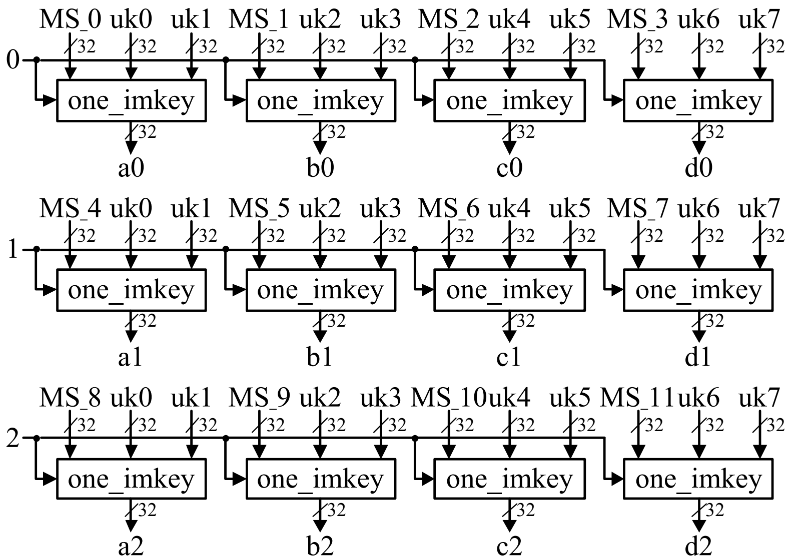


図 6.17 中間鍵生成関数ブロック (全 384 ビット)

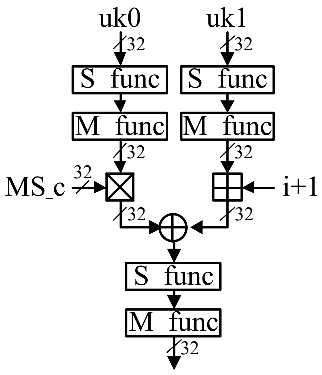


図 6.18　32 ビット中間鍵生成関数ブロック (one_imkey)

拡大鍵生成関数は，図 6.19 に示すように 384 ビットの中間鍵から 32 ビットの拡大鍵を計算する図 6.20 の基本モジュール 4 組で構成され，1 ラウンドあたり 128 ビット，14 ラウンドで 1,792 ビットの拡大鍵を生成する．基本モジュールでは，セレクタ SA~SW により，ラウンド毎に用いる 32 ビット単位の中間鍵を選択する．選択した 128 ビット分の中間鍵に対して，循環シフト，加減算，XOR 演算を行うことにより，32 ビットの拡大鍵を得る．

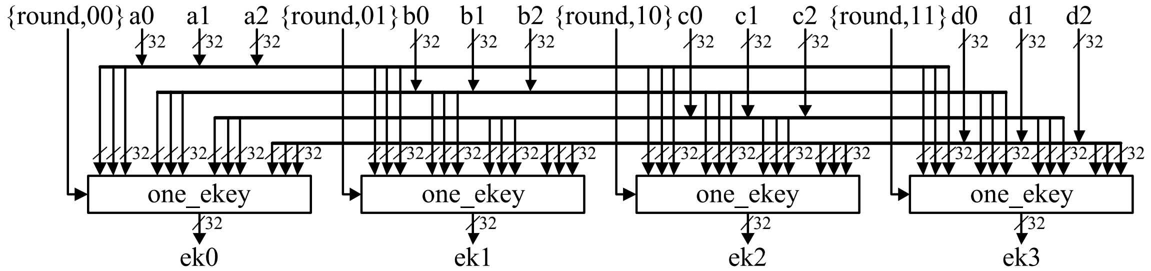


図 6.19　拡大鍵生成関数ブロック (全 128 ビット)

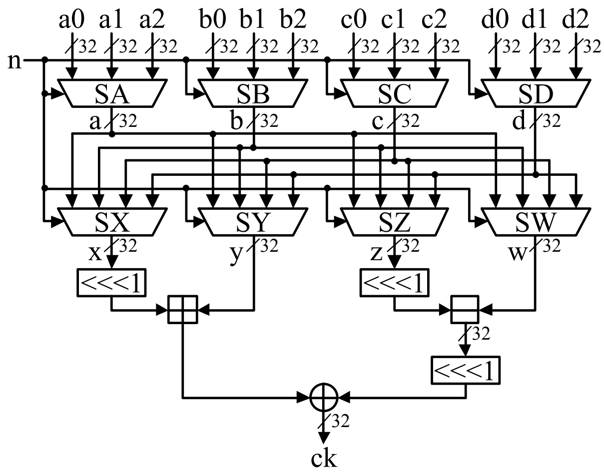


図 6.20　32 ビット拡大鍵生成関数ブロック (one_ekey)

図 6.21 および図 6.22 に暗号化と復号処理のタイミングチャート示す．データ入出力は全てクロックの立ち上がりエッジに同期し，信号の制御は最短のサイクルで行われている．

CLK1: リセット信号 RSTn=0 とすることで，シーケンサーロジックと内部レジスタがクリアされる．

CLK2: イネーブル信号 EN=1，鍵入力用信号 Drdy=1 とすることで，鍵入力ポート Kin 上の秘密鍵 K がマクロの内部鍵レジスタにストアされる．直ちに中間鍵生成処理が開始され，ビジー信号が Busy=1 となる．

CLK17: 中間鍵生成が終了し，鍵が有効となったことを示すステータス信号が Kvld=1 となると同時に Busy=0 に落ちる．

CLK18: Drdy=1，EncDec=0(暗号化モード)となっているため，Din 上のデータ PT が平文としてマクロ内のデータレジスタに取り込まれる．それに伴い，暗号化処理が開始されて Busy=1 となる．

CLK32: 暗号化処理が終了し Busy=0 に落ち，Dvld=1 となり，データ出力ポート Dout に暗号文 CT が出力される．

CLK33: Drdy=1，EncDec=0(暗号化モード)となっているため，Din 上のデータ PT が平文としてマクロ内のデータレジスタに取り込まれる．これにより，次の暗号化処理が開始され，Busy=1 となる．

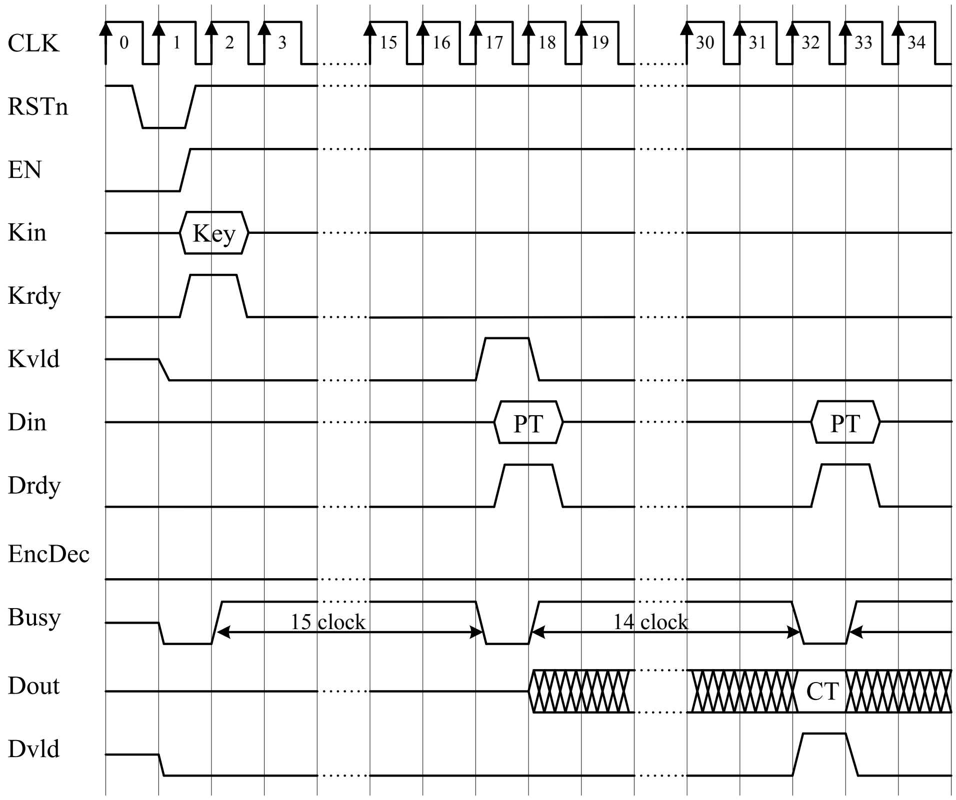


図 6.21 暗号化処理のタイミングチャート

CLK1: リセット信号 RSTn=0 とすることで，シーケンサーロジックと内部レジスタがクリアされる．

CLK2: イネーブル信号 EN=1，鍵入力用信号 Drdy=1 とすることで，鍵入力ポート Kin 上の秘密鍵 K がマクロの内部鍵レジスタにストアされる．直ちに中間鍵生成処理が開始され，ビジー信号が Busy=1 となる．

CLK17: 中間鍵生成が終了し，鍵が有効となったことを示すステータス信号が Kvld=1 となると同時に Busy=0 に落ちる．

CLK18: Drdy=1，EncDec=1(復号モード)となっているため，Din 上のデータ CT が暗号文としてマクロ内のデータレジスタに取り込まれる．それに伴い，復号処理が開始されて Busy=1 となる．

CLK32: 復号処理が終了し Busy=0 に落ち，Dvld=1 となり，データ出力ポート Dout に平文 PT が出力される．

CLK33: Drdy=1，EncDec=1(暗号化モード)となっているため，Din 上のデータ CT が暗号文としてマクロ内のデータレジスタに取り込まれる．これにより，次の復号処理が開始され，Busy=1 となる．

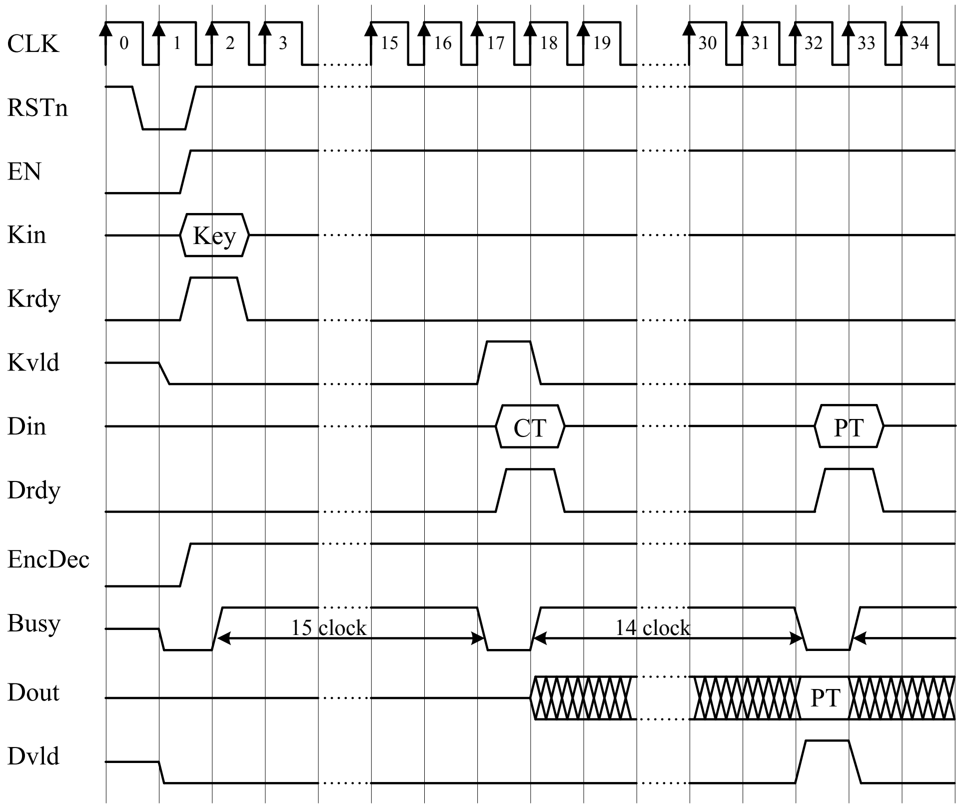


図 6.22 復号処理のタイミングチャート

7. MULTI-S01

MULTI-S01 は，疑似乱数発生器である PANAMA を使用したストリーム暗号で，図 7.1 および図 7.2 に示すように疑似乱数発生部とデータ攪拌部から構成される．PANAMA は暗号化と復号化で共通であり，データ攪拌部は暗号化と復号化で逆変換の関係となっている．

疑似乱数発生器 PANAMA は，reset，push，pull の 3 つのモードを有する．reset モードは，PANAMA のレジスタをクリアし，push モードは疑似乱数生成の初期設定として 256 ビット(8 ワード)の秘密鍵 K，256 ビット(8 ワード)の初期値 Q を内部レジスタにセットする．また pull モードは，初期化された値を用いて疑似乱数を生成する．なおここで，1 ワードは 32 ビットである．

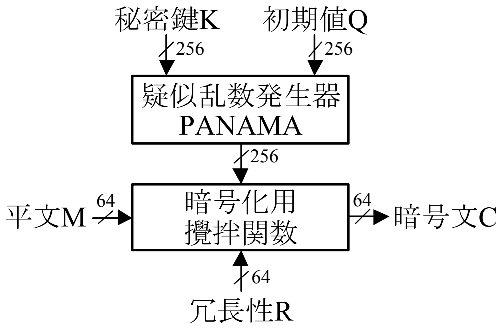


図 7.1　MULTI-S01 の暗号化処理　　図 7.2　MULTI-S01 の復号処理

図 7.3 に PANAMA のデータパスを示す．主レジスタ a は，32 ビット×17 ワードの合計 544 ビットのレジスタで構成される．主レジスタ a をブロックメモリではなく，レジスタに割り当てて 1 ロックでの読み書きを可能とする．また，副レジスタ b は図 7.4 に示すように，32 ビット×8 ワードの LFSR として構成されている．25 ワード入力 17 ワード出力の非線形変換 ρ の構成は図 7.5 の通りである．

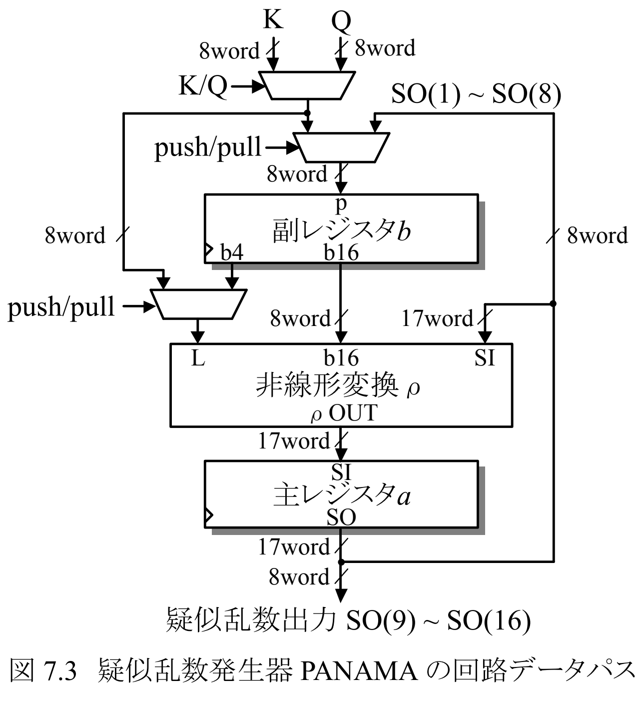


図 7.3　疑似乱数発生器 PANAMA の回路データパス

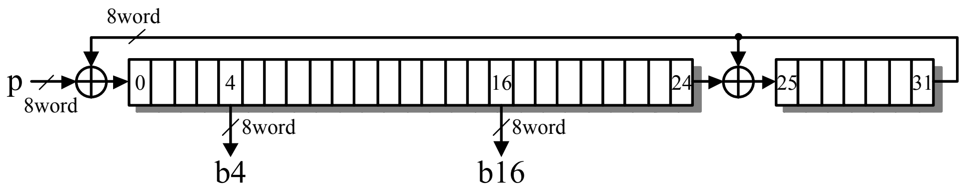


図 7.4 PANAMA の副レジスタ b の構成

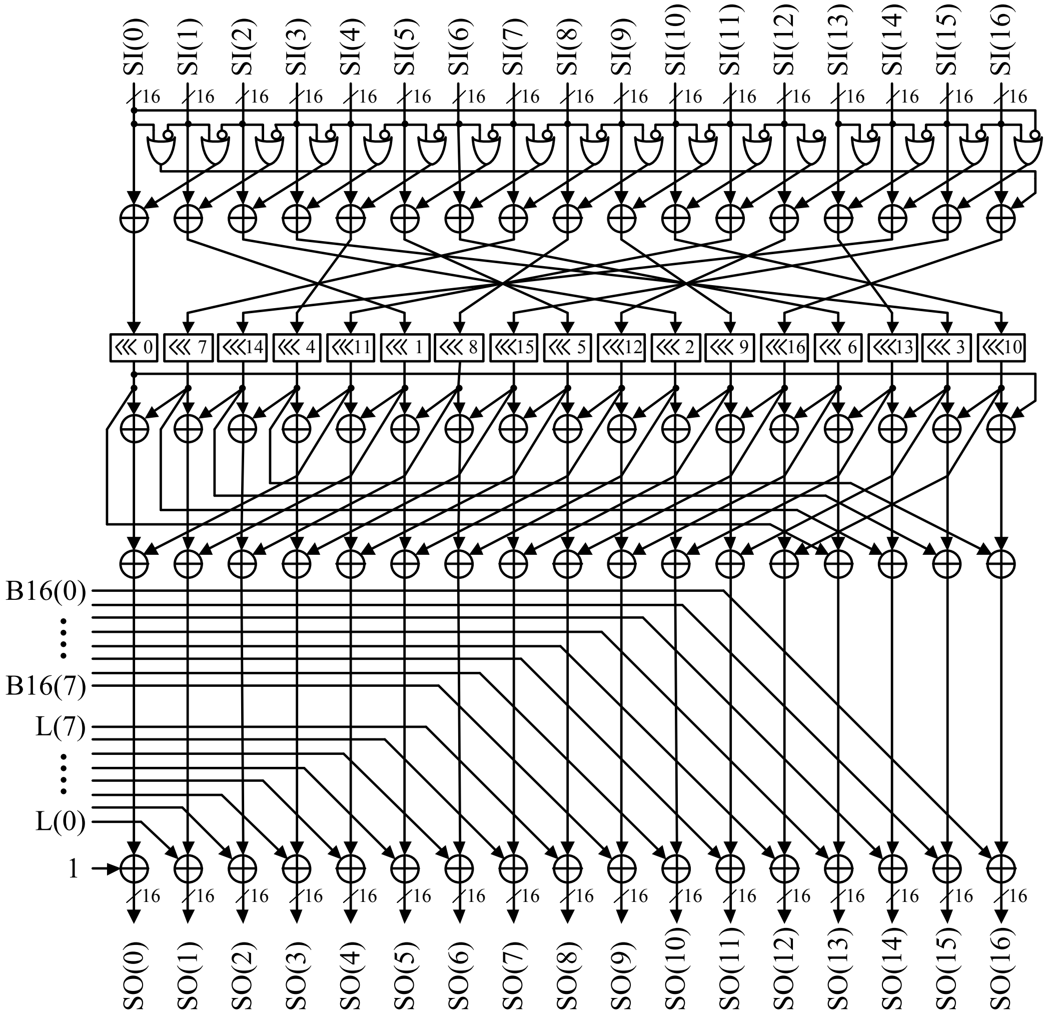


図 7.5 非線形変換 ρ のデータパス

図 7.6 および図 7.7 にそれぞれ暗号化と復号化の 64 ビット入出力の撹拌関数のデータパスを示す. 疑似乱数発生器 PANAMA からの出力を使用して 64 ビットの平文 M を 64 ビットの暗号文 C に暗号化する, あるいは暗号文 C を平文 M に復号化する. P レジスタから C レジスタまでの処理は, 1 クロックで行うため, 毎クロックごとに 64 ビットの平文または暗号文の処理が可能である.

表 7.1 MULTI-S01 暗号マクロの入出力ポート

ポート名	方向	I/O 数	機能
RSTn	In	1	リセット信号．RSTn=0 で，シーケンサおよび内部レジスタをリセットする．リセットは，全ての処理に対して優先され，“CLK”が入力されている限り現在実行中の処理も強制終了する．
CLK	In	1	システムクロック信号．暗号マクロを動作させるためのクロックで，全てのレジスタはこのクロックの立ち上りエッジに同期して動作する．
Kin	In	256	鍵入力ポート．256 ビットの秘密鍵を入力する．
Qin	In	256	乱数列番号入力ポート．256 ビットの乱数列番号を入力する．
Lin	In	32	データブロックレングス入力ポート．32 ビットのデータブロックレングスを入力する．
Din	In	64	データ入力ポート．64 ビットの平文，暗号文を入力する．
Krdy	In	1	鍵レディ入力．“Kin”ポートに秘密鍵が入力されたことを示す．EN=1 の時に Krdy=1 とすることで，“Kin”ポートから秘密鍵が取り込まれ，鍵の事前生成処理が開始される．
Lrdy	In	1	データブロックレングスレディ入力．Lrdy=1 とすることで，“Lin”ポートからデータブロックレングスが取り込まれ，内部レジスタにセットされる．
Drdy	In	1	データレディ入力．“Din”ポートに平文または暗号文が入力されたことを示す．EN=1 の時に Drdy=1 とすることで，“Din”ポートから平文または暗号文が取り込まれ，暗号化，復号化処理が開始される．
EncDec	In	1	暗号，復号処理選択．EncDec=0 の時に暗号化処理，EncDec=1 の時，に復号処理が行われる．
EN	In	1	イネーブル信号．EN=1 の時に処理を行うことができる．EN=1 の時，“Krdy”，“Drdy”を入力しても処理は行われない．
Dout	Out	64	データ出力ポート．暗号化，および復号化が終了した暗号文，平文を出力するポート．Dvad=1 の間が有効なデータである．
Busy	Out	1	ビジー信号．“Krdy”，“Drdy”入力で暗号マクロが処理をしていることを示す信号．Buy=1 の間は“Krdy”，“Drdy”を受け付けることはできない．
Dvld	Out	1	データ出力信号．暗号化，または復号化処理が終了して“Dout”ポートに暗号文，または平文が出力されたことを示す信号．“Dvld”信号は，処理が終了した時点で 1 クロックだけアクティブになる．
Kvld	Out	1	鍵処理終了．秘密鍵の事前再生処理が終了したことを示す信号．“Kvld”信号は，鍵生成が終了した時点で 1 クロックだけアクティブになる．

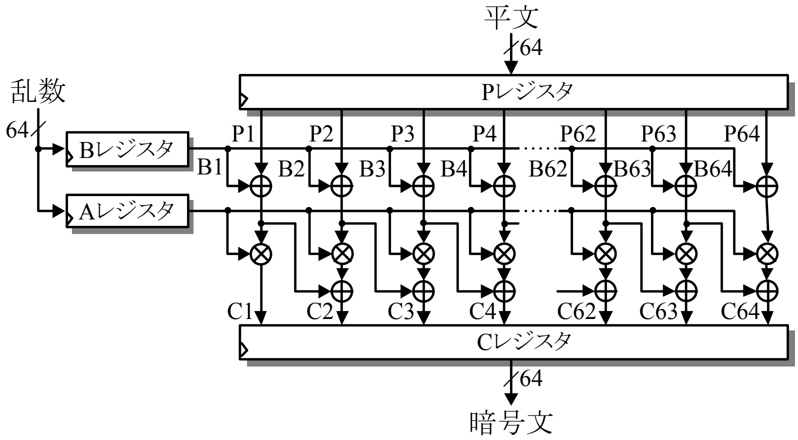


図 7.6　暗号化用撹拌関数ブロック

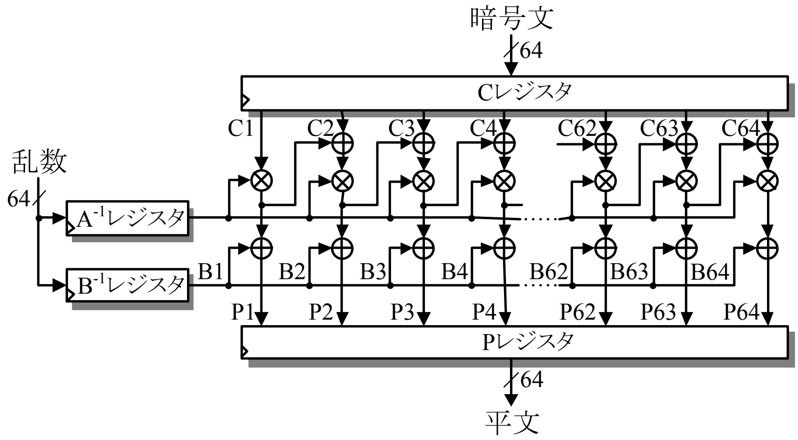


図 7.7　復号化用撹拌関数ブロック

図 7.8 と 7.9 にそれぞれ，暗号化と復号処理のタイミングチャートを示す．データ入出力は全てクロックの立ち上がりエッジに同期し，信号の制御は最短のサイクルで行われている．

CLK1：リセット信号 RSTn=0 とすることで，シーケンサーロジック部とレジスタが初期化される．

CLK2：乱数列番号入力ポート Qin に乱数列番号 Q，鍵入力ポート Kin に秘密鍵 Key をセットして，イネーブル信号 EN=1，鍵レディ信号 Krdy=1 とすることで，秘密鍵が取り込まれ鍵生成処理が開始されビジー信号 Busy=1 となる．

CLK39：鍵生成処理が終了したことを示す鍵処理終了信号 Kvld=1 が 1 クロックだけ出力され，同時にビジー信号 Busy=0 となる．

CLK41：データブロックレングス入力ポート Lin にデータブロックレングス Len をセットし，レングスレディ信号 Lrdy=1 とすることで，レングスが内部レジスタに取り込まれる．

CLK42：64 ビットの平文 PT をデータ入力ポート Din にセットし，暗号化・復号処理選択信号 EncDec=0，データレディ信号 Drdy=1 とすることで，暗号化処理が開始され，Busy=1 となる．

CLK46：暗号化処理が終了し，データ出力信号 Dvld=1，同時に Busy=0 となり，64 ビットの暗号文 CT がデータ出力ポート Dout に出力される．

CLK47：次の平文の入力が可能となる．

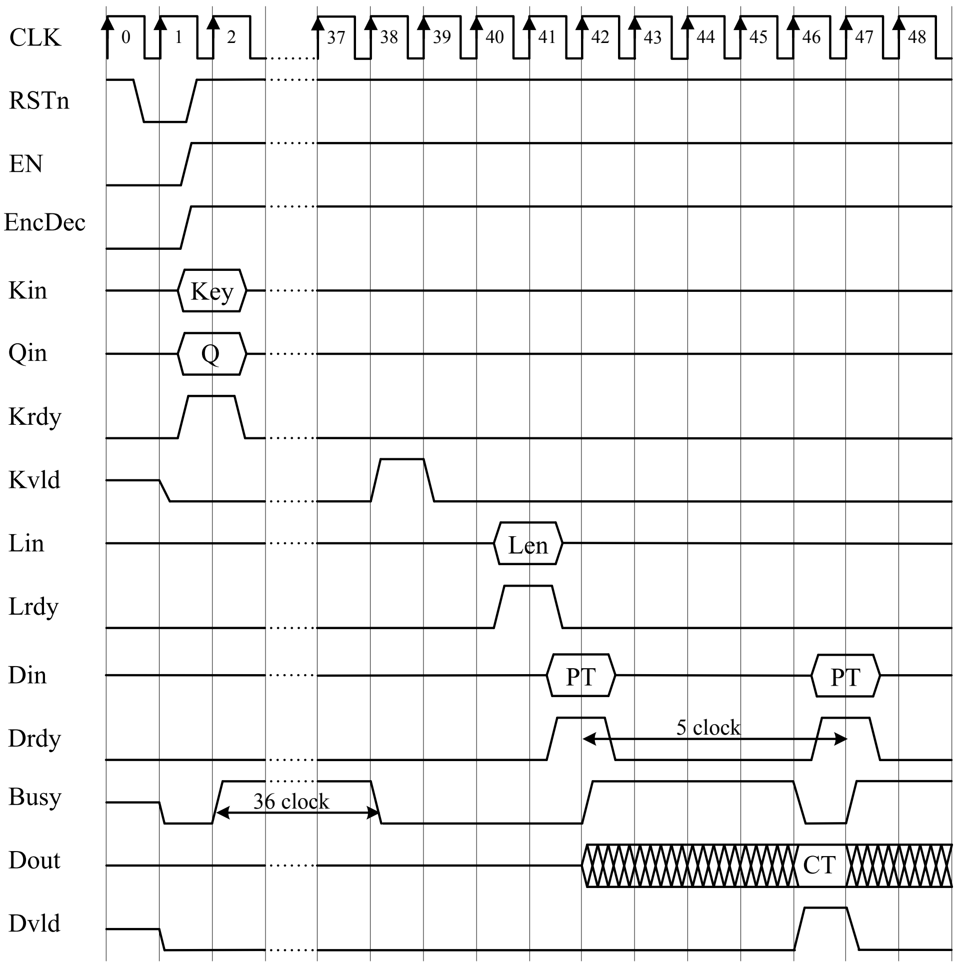


図 7.8　暗号化処理のタイミングチャート

CLK1：リセット信号 RSTn=0 とすることで，シーケンサーロジック部とレジスタが初期化される．

CLK2：乱数列番号入力ポートQinに乱数列番号Q，鍵入力ポートKinに秘密鍵Keyをセットして，イネーブル信号 EN=1，鍵レディ信号 Krdy=1 とすることで，秘密鍵が取り込まれ鍵生成処理が開始されビジー信号 Busy=1 となる．

CLK39：鍵生成処理が終了したことを示す鍵処理終了信号 Kvld=1 が 1 クロックだけ出力され，同時にビジー信号 Busy=0 となる．

CLK41：データブロックレングス入力ポート Lin にデータブロックレングス Len をセットし，レングスレディ信号 Lrdy=1 とすることで，レングスが内部レジスタに取り込まれる．

CLK42：64 ビットの暗号文 CT をデータ入力ポート Din にセットし，暗号化，復号処理選択信号 EncDec=0，データレディ信号 Drdy=1 とすることで，復号処理が開始され，Busy=1 となる．

CLK46：復号処理が終了し，データ処理終了信号 Dvld=1，同時に Busy=0 となり，64 ビットの平文 PT がデータ出力ポート Dout に出力される．

CLK47：次の平文の入力ができる．

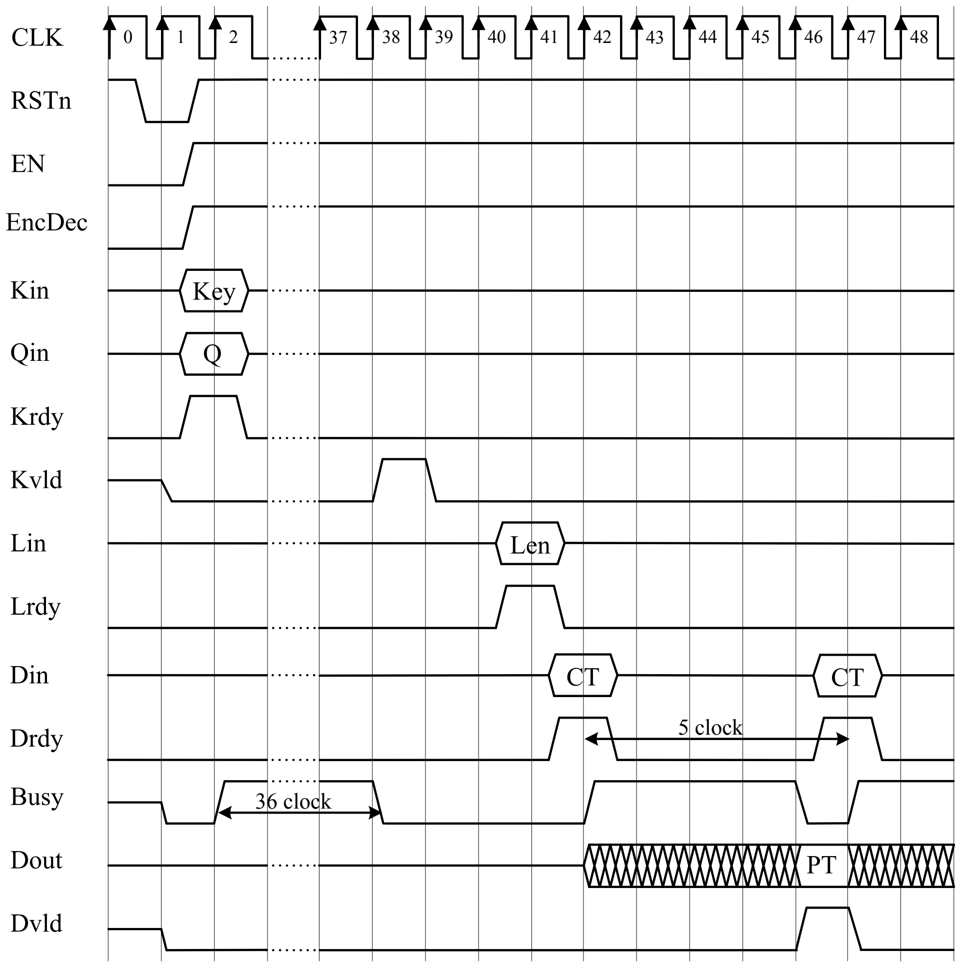


図 7.9 暗号化処理のタイミングチャート

8. MUGI

図 8.1 に MUGI の鍵ストリーム生成器のデータパスを，また図 8.2 および図 8.3 にそれぞれ λ 関数と ρ 関数のデータパスを示す．全レジスタを 1 クロックで読み書きできる構造とし，64 ビットの乱数を 1 クロックごとに出力する．

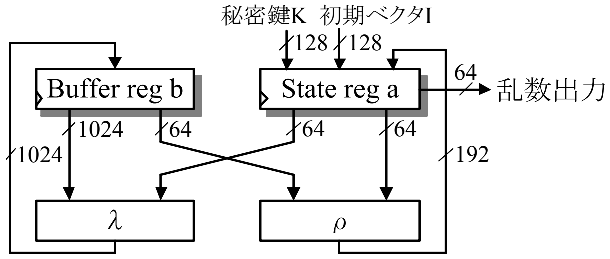


図 8.1 MUGI 回路のデータパス

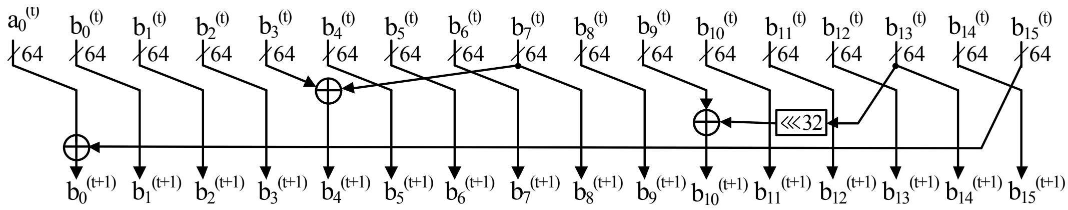


図 8.2 λ 関数ブロック

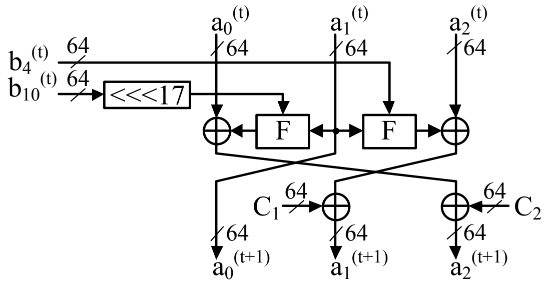


図 8.3 ρ 関数ブロック

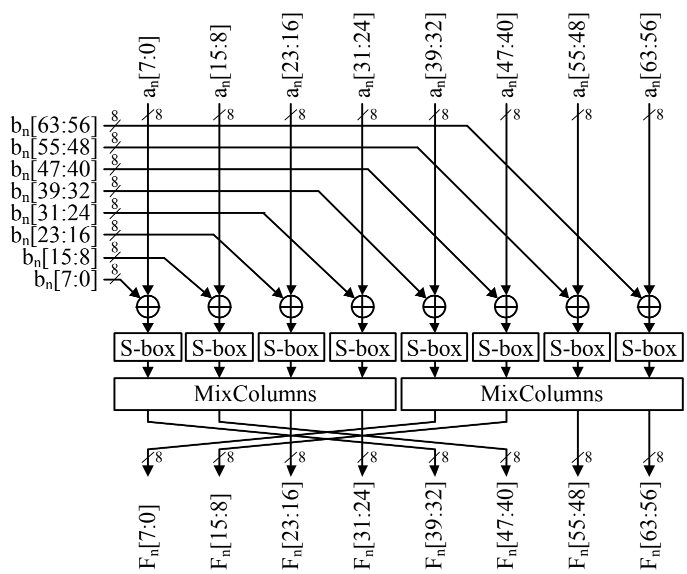


図 8.4 F 関数ブロック

ρ 関数で使用される F 関数は，S-box を用いた非線形変換と MixCloumns を用いた行列変換，バイト置換の組み合わせで定義される. このデータパスを図 8.4 に示す.

表 8.1 MUGI 暗号マクロの入出力ポート

ポート名	方向	I/O 数	機能
RSTn	In	1	リセット信号. RSTn=0 で，シーケンサおよび内部レジスタをリセットする. リセットは，全ての処理に対して優先され，“CLK”が入力されている限り現在実行中の処理も強制終了する.
CLK	In	1	システムクロック信号. 暗号マクロを動作させるためのクロックで，全てのレジスタはこのクロックの立ち上りエッジに同期して動作する.
Kin	In	256	鍵入力ポート. 256 ビットの秘密鍵を入力する.
Iin	In	256	イニシャルベクタ入力ポート 256 ビットのイニシャルベクタを入力する.
Krdy	In	1	鍵レディ入力. “Kin”ポートに秘密鍵が入力されたことを示す. EN=1 の時に Krdy=1 とすることにより“Kin”ポートより秘密鍵を取りこみ，鍵の事前生成処理が開始される.
Irdy	In	1	イニシャルベクタレディ入力. “Iin”ポートにイニシャルベクタが入力されたことを示す. EN=1 の時に Irdy=1 とすることにで，“Iin”ポートよりイニシャルベクタが取り込まれ，内部レジスタにセットされる.
Rrdy	In	1	乱数生成信号. EN=1 の時に Rrdy=1 とすることで，毎クロック，内部ステートが 1 ずつ進み，Rout に新たな乱数が出力される.
EN	In	1	イネーブル信号. EN=1 の時に処理を行うことができる. EN=0 の時は“Krdy”，“Irdy”，“Rrdy”のいずれに入力しても処理は行われない.
Rout	Out	128	乱数データ出力ポート. Rvld=1 の間が有効なデータである.
Busy	Out	1	ビジー信号. “Krdy”，“Irdy”の入力により暗号マクロが処理を実行していることを示す信号. Busy=1 の間は“Krdy”，“Irdy”を受け付けない.
Rvld	Out	1	乱数データ処理終了. “Rout”ポートに乱数データが出力されたお琴を示す信号. 新しい乱数が生成される毎に 1 クロックだけ Rvld=1 となる.
Kvld	Out	1	鍵処理終了. 秘密鍵の事前再生処理が終了したことを示す信号. 鍵生成が終了した時に 1 クロックだけ Kvld=1 となる.

図 8.5 に乱数生成処理のタイミングチャートを示す. データ入出力は全てクロックの立ち上がりエッジに同期し，信号の制御は最短のサイクルで行われている.

CLK1: リセット信号 RSTn=0 とすることで，シーケンサーロジック部とレジスタが初期化される.
CLK2:鍵入力 Kin に秘密鍵 Key をセットして，イネーブル信号 EN=1，鍵レディ信号 Krdy=1 とする

ことで，秘密鍵が取り込まれ鍵生成処理が開始されビジー信号 Busy=1 となる．

CLK19：鍵生成処理が終了したことを示す鍵処理終了信号 Kvld=1 が 1 クロックだけ出力され，同時にビジー信号 Busy=0 となる．

CLK20：イニシャルベクタ入力ポート Iin に 128 ビットのイニシャルベクタ IV をセットし，イニシャルベクタレディ信号 Irdy=1 とすることで，イニシャルベクタ処理が開始され，Busy=1 となる．

CLK52：イニシャルベクタ処理が終了し Busy=0 となる．

CLK53： 乱数生成信号 Rrdy=1 とすることで乱数生成処理が開始され，Busy=1 となる．

CLK54：乱数生成処理終了し，乱数出力信号 Rvld=1，同時に Busy=0 となり，64 ビットの乱数 R0 がポート Rout に出力される．

CLK55：次の乱数を出力するために，再び Rrdy=1 にする．ビジー信号が Busy=1 となる．

CLK56：Rvld=1 となり，乱数 R2 が出力される．

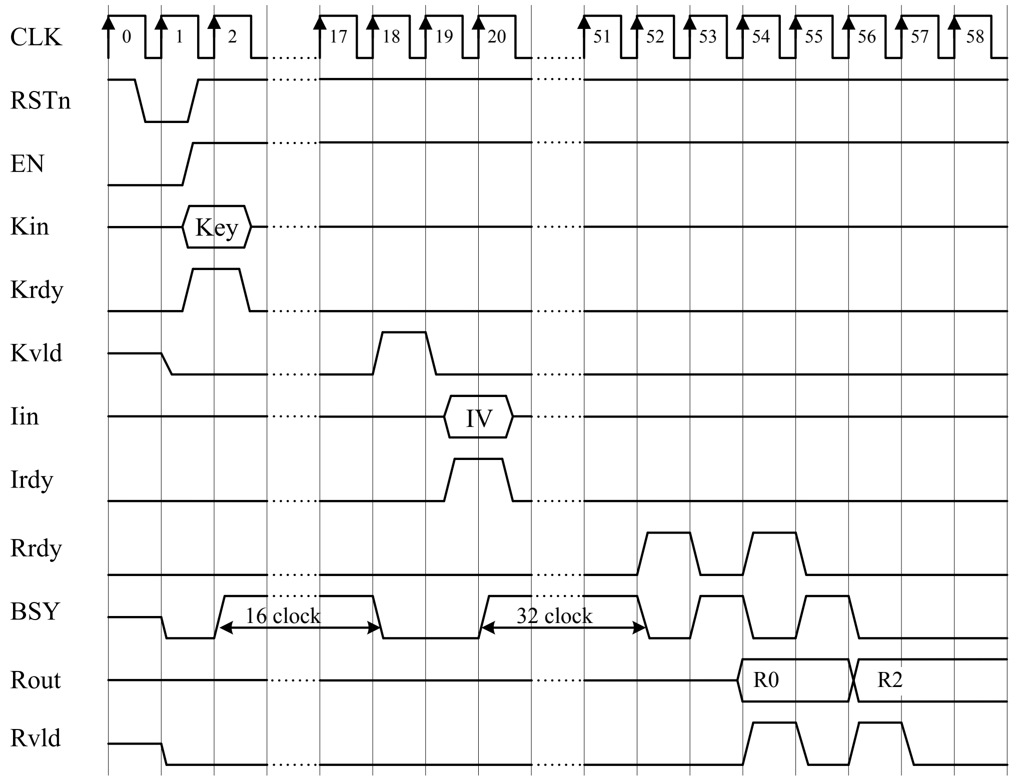


図 8.5 乱数生成処理のタイミングチャート